Downloaded from http://www.everyspec.com

U.S. Department of
Homeland Security

United States
Coast Guard

MANAGEMENT OF SCIENTIFIC AND TECHNICAL INFORMATION (STINFO)

COMDTINST M5260.6

Distribution Statement A: Approved for public release. Distribution is unlimited.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

U.S. Department of Homeland Security
United States Coast Guard

Commandant
Coast Guard Headquarters

2100 2nd ST SW STOP 7901
WASHINGTON DC 20593-7901
Staff Symbol: CG-441
Phone: 202 475 5658
Fax: 202 475 5955

NOV 24 2009

COMDTINST M5260.6

COMMANDANT INSTRUCTION M5260.6

Subj: MANAGEMENT OF SCIENTIFIC AND TECHNICAL INFORMATION (STINFO)

Ref:
(a) Distribution Statements on Technical Orders, DoDD 5230.24
(b) Withholding of Unclassified Technical Data From Public Disclosure, DoDD 5230.25
(c) Air Force Inspection Agency Eagle Look-Scientific and Technical Information (STINFO)
(d) U.S. Code 22 USC Sec. 2778, 2779, 2780, 2785 and 2794
(e) The Coast Guard Freedom of Information and Privacy Acts Manual, COMDTINST M5260.3(series)
(f) Information Assurance Manual, COMDTINST 5500.13 (series)
(g) Safeguarding Sensitive But Unclassified Information, DHS MD Number 11042.1

1. PURPOSE. This Manual promulgates the Standardized Scientific and Technical Information (STINFO) Markings for both Headquarters and the field. In accordance with references (a) through (g), the purpose of the manual establishes a standard and institutionalized program for anyone who uses, originates, reviews, or assigns distribution statements, export-control warnings, intellectual property statements or destruction notices (Standardized STINFO Markings) to information containing STINFO.

2. ACTION. All Coast Guard unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants, and chiefs of headquarters staff elements shall comply with the provisions of this Manual. Internet release is authorized.

3. DIRECTIVES AFFECTED. None.

4. ENVIRONMENTAL ASPECTS AND IMPACT CONSIDERATIONS. Environmental considerations were examined in the development of this instruction and have been determined to be not applicable.

5. FORMS/REPORTS. None.

DISTRIBUTION – SDL No. 154

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	1				1								1		1	1			1							
B																										
C																										
D																							1			
E																										
F																										
G																										
H																										

NON-STANDARD DISTRIBUTION:

Downloaded from http://www.everyspec.com

6. REQUESTS FOR CHANGES. Recommendations for changes and improvements to the Management of Scientific and Technical Information (STINFO), COMDTINST 5260.6 (series) will be submitted via the chain of command to Commandant (CG-441).

T. P. OSTEBO /s/
Rear Admiral, U. S. Coast Guard
Assistant Commandant for Engineering and Logistics

Downloaded from http://www.everyspec.com

TABLE OF CONTENTS

CHAPTER 1 OVERVIEW

A.	General	1-1
B.	Discussion	1-1
C.	Instruction Guidelines	1-1
D.	STINFO Authority	1-1

CHAPTER 2 STINFO USER

A.	General	2-1
B.	Resources	2-4

CHAPTER 3 ORIGINATOR, DEVELOPER, AND PUBLISHER OF STINFO

A.	STINFO Marking Authority	3-1
B.	Responsibilities	3-1
C.	Mandatory Markings on STINFO	3-2
D.	Freedom of Information Act (FOIA) and Privacy Act (PA)	3-4
E.	Automated Information System (AIS)	3-5

CHAPTER 4 STINFO ACCESS AND SECURITY

A.	General	4-1
B.	Authorized Access to STINFO	4-1
C.	Inadvertent Release or Compromise of Controlled STINFO	4-2

CHAPTER 5 CONTRACTING AND TRAINING REQUIREMENTS

A.	Contracting	5-1
B.	Training	5-1
C.	Forms/Reports	5-1

APPENDIX A References

ENCLOSURES
(1) Placement of Standardized STINFO Markings
(2) Standardized STINFO Distribution Statements
(3) Full Export-Control Warning Statement
(4) Distribution Statement Matrix
(5) Ten Reasons for Distribution Statement Restrictions
(6) DHS Non-Disclosure Agreement
(7) Example of Unit Level STINFO Reviewer Designation Letter

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

CHAPTER 1. OVERVIEW

A. General. Scientific and Technical Information (STINFO) is defined as all communicable classified and unclassified limited-access information that relates to military operations and systems including:

1. Research, development, engineering, testing, evaluation, production, logistics, and operations.
2. Information that can be used to design, procure, support, maintain, repair or overhaul; products, services, and equipment.

B. Discussion. In accordance with the Department of Defense Directive (DoDD) 3200.12, the Department of Defense (DoD) and Defense Technical Information Center (DTIC) have been reviewing, standardizing, and institutionalizing the methods of creating, marking, acquiring, securing, handling, archiving, and the dissemination of STINFO. This requirement became paramount after the terrorist attacks on 11 September 2001 and the thefts of government computers and equipment. STINFO includes all types of technical data in numerous formats including draft/working/hard copy, digital and electronic documents. The unauthorized use, distribution, or replication of certain information under the Copyright, Patent, Intellectual Property (IP), Arms Export-Control Act (AECA), and Export Administration Act (EAA) imposes significant fines, civil liabilities, criminal penalties, and administrative actions in accordance with Public Law and Executive Orders. On the other hand, withholding information subject to release under the Freedom of Information Act (FOIA) and Privacy Act may result in severe penalties and consequences. Applying the correct Standardized STINFO Markings to all required documents and/or information is essential in order to preclude the agency, service, or customer from significant liability and possibly affecting the national security of the country.

C. Instruction Guidelines. This instruction addresses important security and standardization issues of which the end-user, originator, developer, and publisher of information requiring a limited distribution or access will need to be cognizant. Chapter 2 of this instruction is designed to provide the end-user of STINFO with an overview of the STINFO program and the necessary actions required when utilizing the information. The remaining chapters of this Commandant Instruction will assist the Unit FOIA Officer, Aviation Logistics Center (ALC) STINFO Program Manager, Unit Level STINFO Reviewer, originator, developer, and publisher of STINFO with the knowledge required for the assignment of the Standardized STINFO Markings for unclassified limited-access information.

D. STINFO Authority. The overarching authority of the Coast Guard (CG) STINFO program is the Assistant Commandant for Engineering and Logistics, Commandant (CG-4). The program is managed by the STINFO Program Manager at ALC.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

CHAPTER 2. STINFO USER

A. General

1. End User. The key word for all end-users of STINFO is **AWARENESS**. All STINFO will be labeled with very important information, allowing the end-user to know who is authorized to view/use the information and what to do with that information when the document is no longer required. All of the pertinent information is readily available on the cover or front page of all written technical documents (manuals, papers, reports). The informative data will also be located on electronic storage units (CD, DVD, portable hard drives, floppies, etc.) and their protective covers, as well as on the first slide of an electronic presentation or briefing (see Enclosure (1)).

   STINFO can be categorized with a Security Classification (Top Secret, Secret, or Confidential), as unclassified but having a limited-access, or unclassified and available to the public. This Instruction will concentrate on the STINFO that is unclassified but having a limited-access.

   The term "For Official Use Only" (FOUO) is not considered a Security Classification even though the data has a limited-access restriction and is only available on a need-to-know basis. The designation of FOUO on a document only applies to information applicable to the FOIA and Privacy Acts.

   The Department of Homeland Security (DHS) and CG require all contracted companies as well as their employees to sign a Non-Disclosure Agreement (NDA) (DHS Form 11000-6) prior to starting work for the government in accordance with DHS MD 11402.1. This document allows authorized contractors access to the necessary information required for the purpose of performing their contracted duties.

2. All unclassified and unclassified limited-access STINFO not protected by the FOIA or Privacy Acts (PA), or listed as an exception in Chapter 2.A.2, will be marked with the Standardized STINFO Markings which consists of a Distribution Statement, Export-Control Warning Statement (if applicable) and a Destruction Notice. STINFO should also be marked with an Intellectual Property (Proprietary Information) Notice (if applicable). See Enclosure (1), Enclosure (2), and Chapter 2.A.2.d.

   a. Distribution Statement. Identifies who or what audience is authorized to view and or use the information (see Enclosure (2)). All end-users of STINFO are required to ensure that the security of the information is maintained by only allowing access to those eligible per the Distribution Statement.

   b. Export-Control Warning Statement (if applicable). Numerous Public Laws and Executive Orders specify who can and cannot have access to unclassified limited-access STINFO. Allowing the wrong individuals access can affect the security of our country. The U.S. Munitions List (USML) and Commerce Control List (CCL) define what types of equipment and related information that cannot be exported or released to unauthorized entities. The USML specifically states any information pertaining to CG surface vessels as well as any aircraft used by the military may not be unlawfully exported.

Downloaded from http://www.everyspec.com

Care should be taken to ensure that you are not unintentionally exporting limited-access STINFO as the definition of exporting can be confusing (see 22 U.S.C. Sec. 2794). Here are just some examples that can be interpreted as exporting information:

(1) The topic of a briefing or presentation is beyond the security or access limits of those in attendance.

(2) Allowing enrollment in formal training and correspondence courses by unauthorized audiences.

(3) Allowing access by an unauthorized individual to either complete or partial limited-access information such as removed pages from a technical document/manual or the maintenance instruction portion of an Asset Computerized Maintenance System Card (ACMS).

(4) E-mailing a limited-access document to unauthorized individuals.

(5) Communicating limited-access information to unauthorized individuals.

Allowing this information to be obtained by the wrong person(s) can result in serious fines and penalties toward an individual and/or agency, including imprisonment up to 10 years and fines up to $1,000,000 or both (see Enclosure (3), Full Export-Control Warning Statement). Export-Controlled STINFO may only be handled by and disclosed to those individuals listed in Chapter 4.B.2 and 4.B.3. Contractors, as well as those individuals not contracted with the U.S. Government, are required to be registered and licensed with the U.S. Government which only then allows access to Export-Controlled information on a need to know basis. Registration for Export-Controlled information does not, however, include access to information that is also annotated with a Proprietary Information Notice, unless the individual is actually employed by the entity that owns the information or written permission has been received authorizing its release. See paragraph 2.A.2.d below for more information. Releasing export-controlled STINFO to an authorized agent outside of the U.S. Government must contain the Full Export-Control Warning Statement as shown in Enclosure (3).

c. Destruction Notice. All classified or limited-access STINFO will be marked with a destruction notice. The security of a document carries through its origin, use, storage, and final disposition. The destruction requirements of unclassified limited-access STINFO can even include items such as the removed pages from a change or revision to a technical manual, the maintenance instruction sheets after the completion of an ACMS task, used hard drives, CDs, DVDs, or Floppy Disks, or handouts that are left over from a presentation. Allowing an unauthorized individual access to a partial document containing information that is Export-Controlled can place the custodian of the information in the position of compromising data that is included on one of the lists annotated above in paragraph 2.A.2.b, and thereby in violation of Public Laws and Executive Orders.

The preferred method of disposal of unclassified limited-access STINFO (Distribution Statement B, C, D, E, and F) is by shredding or by destruction in a manner whereby the document cannot be reconstructed. See Enclosure (2) for an

Downloaded from http://www.everyspec.com

example of the actual destruction notice. Proprietary STINFO must be shredded. The destruction methods described below may only be used with Department of Homeland Security (DHS) DHS/CG/DoD unclassified limited-access STINFO when the availability of a shredder is not available.

(1) Placing non-sequential pages of a document in different recycling or waste bins
(2) Tearing pages into three or more pieces and placing them in a single bin
(3) Burning

d. Intellectual Property (Proprietary Information) Notice (if applicable). Owners of IP STINFO will negotiate with government specific rights for the use of their information during the contracting phase of a proposal. The owner of the information is required to label their technical documents with the negotiated rights for the use of the information. Failing to annotate a document with the negotiated rights will automatically allow the government unlimited right to the information.

Extreme care must be taken if there is a possibility that the information could become available to an unauthorized person or entity such as another contractor from a competing company not contracted with DHS/CG/DoD. Allowing STINFO to be released without written permission from the owner can result in significant fines from civil lawsuits to the individual and entity releasing the information, and the possible lack of future technical support from the owner of the document.

Written permission must be obtained prior to the use of data containing a Copyright. New laws place the responsibility of researching material that may have a Copyright on the user instead of the author of the information. Information either produced or funded by the government will normally contain copyrighted material with a pre-negotiated government–use license. Extreme care and diligence should be taken prior to making a copy of an existing document, drawing, or illustration for use in a CG/DoD publication.

The DHS and CG require all contracted companies as well as their employees to sign a Non-Disclosure Agreement (NDA) (DHS Form 11000-6) prior to starting work for the government in accordance with DHS MD 11402. This document allows authorized contactors access to the necessary information required for the purpose of performing their contracted duties.

e. Any legacy STINFO received without the Standardized STINFO Markings with a publication date prior to the date of this instruction shall be handled as if being marked with a Distribution Statement D (CG/DoD and their Contractors). Most new documents received without the Standardized STINFO Markings are done so inadvertently due to oversight or without the knowledge that the markings are required. The new STINFO shall be returned to the Originator in order to assign the Standardized STINFO Markings prior to any further distribution.

3. Exceptions to the STINFO Marking Rule. Certain documents do not require the Standardized STINFO Markings including:

a. Technical proposals or similar documents submitted by contractors seeking DoD funds or contracts.

Downloaded from http://www.everyspec.com

b. Personnel records, administrative papers, or procedural directives internal to a division within a command.

c. Catalogs and brochures, directories, promotional materials, and contract administration documents; or technical documents used by CG/DoD that have not been produced by or for the CG/DoD such as a book of industry standards or a privately published scientific journal.

d. Approved standard forms (CG, DoD, etc.).

e. Technical documents categorized by the National Security Agency (NSA) as cryptographic and communications security or communications and electronic intelligence.

B. Resources.

1. Numerous resources are available to the end-user of STINFO, including the unit FOIA, Public Affairs Officer (PAO), Security Officer, Unit STINFO Reviewer, Originator, and the CG STINFO Program Manager at ALC.

2. More in-depth discussion and instructions on the marking of STINFO can be found in the Standardized STINFO Markings Process Guide, CGTO PG-85-00-290, which is available electronically on the ALC Engineering Services Division (ESD) Aircraft Publications website.

3. Please refer to the subsequent chapters and Appendix A for more in-depth information on the application for the CG STINFO policy.

4. The Information and Life Cycle Management Manual, COMDTINST M5212.12 (series).

Downloaded from http://www.everyspec.com

CHAPTER 3. ORGINATOR, DEVELOPER, AND PUBLISHER OF STINFO

A. STINFO Marking Authority.

1. The Assistant Commandant for Engineering and Logistics, Commandant (CG-4), has the overarching authority for the CG STINFO program.

2. The ALC is designated as the STINFO Center of Excellence. The STINFO Program Manager is the managing authority for the CG STINFO Program; ensuring standardization, oversight, and implementation of the Standardized STINFO Markings. See Enclosure (1).

B. Responsibilities.

1. Unit Commanding Officer (Controlling Office). The Unit Commanding Officer or his/her designated representative (Example: FOIA Officer, PAO, Unit STINFO Reviewer) responsible for the origination of the origination of the technical document has the overall responsibility for assuring that required reviews are completed and the appropriate Standardized STINFO Markings are assigned.

2. Originator. Any originator who believes STINFO should be classified (Top Secret, Secret, Confidential) shall mark and handle that material at the appropriate level of classification and forward it through the unit Security Officer to an Original Classification Authority (OCA), for final adjudication. Commandant, Assistant Commandant of Operations (ACO), and Assistant Commandant for Intelligence and Criminal Investigations, Commandant (CG-2) are the only three entities within the Coast Guard allowed to classify a document with a Security Classification.

   For unclassified limited-access material, the originator should refer to the Standardized STINFO Markings Process Guide, CGTO PG-85-00-290, and/or request assistance from the unit FOIA Officer and/or PAO in determining whether the document should be available for public release or requires a limited distribution. Under no circumstances will anyone change an existing distribution statement without the consent of the Controlling Office or Originator. All distribution statements other than “A” must contain a reason for the limited distribution (Enclosure (4) and Enclosure (5)). The unit FOIA Officer and/or PAO should be consulted prior to categorizing STINFO with a “Distribution Statement A; Approved for Public Release; Distribution is Unlimited” marking. The originator must ensure that when Standardized STINFO Markings are applied or reapplied, there is a reasonable possibility the information can be protected from unauthorized disclosure.

3. Technical Writer and/or Graphics Illustrator/Technical Draftsperson. These individuals are responsible for the actual placement of the predetermined Standardized STINFO Markings as listed in Enclosure (2) on the STINFO. Any new document without a distribution statement will be returned to the originator with a Distribution Statement F (see Enclosure (2)) until such time that the originator can identify the appropriate audience. Only then will anyone other than the originator have access to the information.

Downloaded from http://www.everyspec.com

4. Automated Information Systems (AIS). DHS/CG/DoD and other government departments or agencies are subject to the security requirements of that department or agency.

5. Contracting Officer's Technical Representative (COTR)/Project Manager (if applicable). The COTR/Project Manager ensures the project results are documented and reviewed, Standardized STINFO Markings are properly assigned, and accepted by the active duty military or government civilian employee authorized to do so. Aviation related documented efforts are forward to the ALC ESD Technical Publications Branch for dissemination. Other non aviation points of contact need to be developed.

6. Unit Security Officer. The unit security officer shall review any document deemed to contain information that should be considered for a security classification (see Originator above).

7. Unit FOIA/PAO Officer. The FOIA Officer should assist the PAO, command/unit Operations and Intelligence Officer or other responsible entities as resources allow to review and approve all proposed tentatively marked "Distribution Statement A, Approved for Public Release; Distribution is Unlimited" STINFO. The exact allocation of unit responsibilities for this function will depend on the distribution of unit resources. The key thing is this function needs to be performed.

8. CG STINFO Program Manager. The STINFO Manager will oversee the CG STINFO program and assist the unit FOIA Officers and originators with its implementation per this instruction. Additional responsibilities include the coordination of STINFO Awareness Training and representing CG interests at STINFO meetings and conferences. The Program Manager is required to have a minimum of a Secret Clearance.

9. Unit Level STINFO Reviewer. The Unit Level STINFO Reviewer will be required at units that may, or will produce, distribute, and/or present information containing, copyrights, intellectual property (proprietary information), patents, trademarks, and/or Export-Controlled information.

C. Mandatory Markings on STINFO. All STINFO shall be marked in a manner whereby the statement will not restrict the data any further than actually required to protect the interests of the U.S. Government. The security classification (if applicable) and Standardized STINFO Markings will be marked on each document or item containing STINFO.

Unmarked STINFO with a publication date prior to the date of this instruction (legacy STINFO) will only be annotated with the Standardized STINFO Markings when the document or item is reviewed, requested, or updated. All unmarked legacy STINFO can only be released to CG/DoD personnel and their Contractors (Distribution Statement D) until it is reviewed and properly marked. Unmarked new STINFO shall be returned to the originator in order to assign the Standardized STINFO Markings prior to any further distribution. All Standardized STINFO Markings will be made as depicted in Enclosure (1) and Enclosure (2). Exceptions to the marking rule are listed in Chapter 2.A.3. The five considerations of the Standardized STINFO Markings are listed below:

Downloaded from http://www.everyspec.com

1. Security Classifications. STINFO is either Classified or Unclassified and marked accordingly.

   a. Classified documents are categorized and marked Top Secret, Secret or Confidential per the Classified Information Management Program, COMDTINST M5510.22 (series), by the Original Classification Authority (see Originator, Chapter 3.B.2).

   b. Unclassified documents can fall into two categories: unclassified and available for public release or unclassified but have limited-access and are controlled. Both categories of documents require the Standardized STINFO Markings. The second category is available to only those with a need-to-know requirement and can be identified by numerous titles or markings (Distribution Statements, FOUO, Sensitive But Unclassified (SBU), Protected Critical Infrastructure Information (PCII), Sensitive Security Information (SSI), etc.), depending on the issuing government agency. Unclassified limited-access information may contain content that is protected under the FOIA, Personal Privacy Act, or is categorized as Export-Controlled by the EAA or AECA. The Controlling Office or Originator must approve any distribution beyond what is assigned.

2. Distribution Statements. A distribution statement is distinct from and in addition to security classification markings and is required on all STINFO. Distribution statements are used to mark STINFO to denote the extent of its availability for a secondary distribution and to whom (see Enclosure (2)). Secondary distribution includes loaning, allowing the reading of, or releasing a document outright, in whole or in part without additional approvals or authorizations by the originator or controlling office. Distribution statements shall be used on all CG/DoD classified and unclassified data to restrict dissemination beyond the limits provided by applying security and need-to-know controls and to control dissemination of the data following declassification. Distribution statements are made up of four distinct pieces of information.

   a. Who is authorized to view the document (Authorized Audience)?
   b. Reason for the restriction: See Enclosure (4) and Enclosure (5).
   c. Identity of the Controlling CG/DoD Office/Originator (Owner).
   d. Date of review or determination for the limited-access.

NOTE

STINFO determined to be available for Public Release (Distribution Statement A) will not have any other restriction, statement, or notice attached to the document/item.

3. Export-Control Warning Statement. Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR) are based on the national security of our country. The export-control warning statement identifies technical documents that contain STINFO subject to withholding from public release without a U.S. Government issued license. All STINFO subject to export-control laws must be marked with the export-control warning statement, the appropriate distribution

Downloaded from http://www.everyspec.com

statement, and destruction notice as listed in Enclosure (2). Any export-controlled document, or portion thereof, disseminated outside of the U.S. Government must contain, in addition to the standard warning statement on the cover, the full Export-Control Act Warning Statement (Enclosure (3)) as a separate cover sheet.

NOTE

The Export-Control Warning Statement is required on all STINFO referenced in the CCL and/or U.S. USML. As an example, the current USML states that all technical information applicable to CG surface vessels as well as any aircraft used by the military is export-controlled. When in doubt, ensure that you refer to the lists for other categories or specific items in question.

EAR/CCL website: http://www.access.gpo.gov/bis/ear/ear_data.html

ITAR/USML website:
http://www.access.gpo.gov/nara/cfr/waisidx_99/22cfr121_99.html

4. Intellectual Property (IP) Notice. These contractor-placed notice specify the IP rights (Unlimited Rights, Limited Rights, Government Purpose Rights, Small Business Innovation and Research (SBIR) Rights, Restricted Rights, Specifically Negotiated License Rights, or pre-existing markings authorized under a previous government contract) attached to the STINFO. An IP Notice prohibits a competing contractor from viewing another contractor's STINFO unless special permission is granted by the owner of the document. IP categories include Trade Secrets, Trademarks, Technical Data, Computer Software, Copyright, and Patents, IP is also known as Proprietary Information. Contracting Officers, Commandant (CG-934), shall ensure each individual contracted by the CG to perform work, as well as the contracted corporation, is required to sign a DHS Non-Disclosure Agreement (DHS Form 11000-6) (Enclosure (6)) prior to starting work in accordance with the DHS Management Directive, Safeguarding Sensitive But Unclassified For Official Use Only Information, DHS MD 11042.1.

   DHS Form 11000-6: http://fas.org/sgp/othergov/dhs-nda.pdf

5. Destruction Notice. These notices dictate the destruction requirements for classified and unclassified but limited-access STINFO (see Enclosure (2)). "Distribution Statement A: Approved for Public Release; Distribution is Unlimited" information has no special destruction requirements and may be discarded in a regular trash can.

   See Chapter 2.A.2.c, for more in-depth information on the approved destruction methods for unclassified limited-access STINFO.

D. FOIA and PA. FOIA specifies that records must be made available to "any person" (including foreign citizens), partnerships, corporations, associations, and foreign, state, or local governments, while PA records may only be made available to the individual whose records are maintained by the Federal government. The definition of "person" does not, however, include other Federal government agencies; therefore, requests for CG records from other Federal agencies are not considered FOIA requests and are not

Downloaded from http://www.everyspec.com

processed under the requirements of the Act. Investigatory material may be shared with state and local law enforcement agencies. The only exception to this broad "any person" standard is for those who flout the law such as a fugitive from justice. Requesters are not required to explain or justify reasons for their requests. Documents that cannot be released due to the restrictions of FOIA or PA will be labeled as FOUO; see Enclosure (2), referencing one of the nine allowed exemptions listed in the CG FOIA and PA Manual, COMDTINST M5260.3 (series). All FOIA requests for unclassified but limited-access information must be reviewed by the originator and the FOIA Officer of the local command and will consult with the Surface Forces Logistics Command or CG Headquarters, Commandant (CG-0944) Legal as the final authority, prior to limiting or denying access to any requested information under FOIA.

E. Automated Information Systems (AIS). Classified and unclassified but limited-access information handled by existing CG automated systems (TIMOS, ALMIS, ATIMS, JEDMICS, CGTIMS, NETIMS) or any developing and/or future automated systems and associated telecommunications shall be properly safeguarded against unauthorized access, use, modification, destruction, or other denial of service through the integrated employment of appropriate physical, personnel, administrative, hardware, software, communications, and emanations security controls.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

CHAPTER 4. STINFO ACCESS AND SECURITY

A. General. All users of STINFO must be cognizant of and adhere to all security classifications, distribution and export-control warning statements, and intellectual property and destruction notices (Standardized STINFO Markings).

B. Authorized Access To STINFO.

1. Classified Information (Top Secret, Secret, Confidential) and FOUO. Classified information may only be released to a person who has at least an equal or greater security clearance than the requested information and then only on a need-to-know basis. FOUO may only be released to those on a need-to-know basis.

2. Active Duty, U.S. Military Reservists, and USCG Auxiliary. May have access to unclassified information with Distribution Codes A, B, C, D, E, and X. Access to Distribution Code F may only be authorized with prior approval from the Controlling Office or originator of the information.

3. Government Employees. May have access to unclassified information with Distribution Codes A, B, C, D, E, and X. Access to Distribution Code F may only be authorized with prior approval from the Controlling Office or Originator of the information.

4. DHS/CG/DoD Contractors. Those U.S. contractors currently holding grants or contracts with the DHS/CG/DoD or those contractors declared eligible for services by a sponsoring DHS/CG/DoD activity on the basis of participation in a DHS/CG/DoD Potential Contractor Program may have access to all unclassified Distribution Code A, C, and D information after signing a DHS Form 11000-6, DHS Non-Disclosure Agreement (Enclosure (6)) which is available at:

   http://www.fas/org/sgp/othergov/dhs-nda.pdf

   The contracting officers will be responsible for ensuring that each contractor understands and signs the non-disclosure agreement prior to starting work.

NOTE

Distribution Statement X will not be used on any CG STINFO. Any DoD STINFO that contains the Distribution X should be handled as Export-Controlled.

C. Inadvertent Release or Compromise of Controlled STINFO.

1. The loss, compromise, suspected compromise, or unauthorized disclosure of classified or unclassified but controlled STINFO will be reported to the unit Security Officer.

2. Suspicious or inappropriate requests for information by any means, e.g., E-mail or verbal, shall be reported to the unit Security Officer.

3. Employees or contractors who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of FOUO information will report it immediately, not later than the next working day, to the originator and unit Security Officer.

Downloaded from http://www.everyspec.com

4. Notification to the unit Security Officer will be made without delay when the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned or ongoing operation.
5. At the request of the originator, an inquiry will be conducted by the unit Security Officer or other designee to determine the cause and effect of the incident and the appropriateness of administrative or disciplinary action against the offender.

Downloaded from http://www.everyspec.com

CHAPTER 5. CONTRACTING AND TRAINING REQUIREMENTS

A. Contracting.

1. Government funded projects or studies requiring research and development, with the results being new technologies or improvements to existing processes, must include as part of their contract, a project status and final report for submission to the DTIC in accordance with DoDD 3200.12. The project COTR will submit the final report with an original DoD SF-298 (http://www.dtic.mil/whs/directives/infomgt/forms/eforms/sf0298.pdf) to the STINFO Project Manager at ALC.

2. All STINFO received by the government in response to a contract award must be marked with the Standardized STINFO Markings (Enclosure (2)). Aviation concurrence of the markings will be conducted by the ALC ESD Technical Publications Branch Chief. Other approval entities will be determined at a future time.

B. Training. All CG military, government, and contractor personnel shall be indoctrinated on STINFO identification, disclosure, protection, dissemination, and destruction in accordance with the information contained within this Commandant Instruction and the STINFO Process Guide, CGTO-PG-85-00-290. Additional training opportunities are available through the Defense Technical Information Center, Ft. Belvior, VA and CG specific Powerpoint presentations. Future awareness training will be available via the CG Learning Portal after development.

C. Forms/Reports. Applicable training records and designation of authority letters will be maintained at the unit level of military and civil service employees. Contractor training records shall be maintained by the respective contractor.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

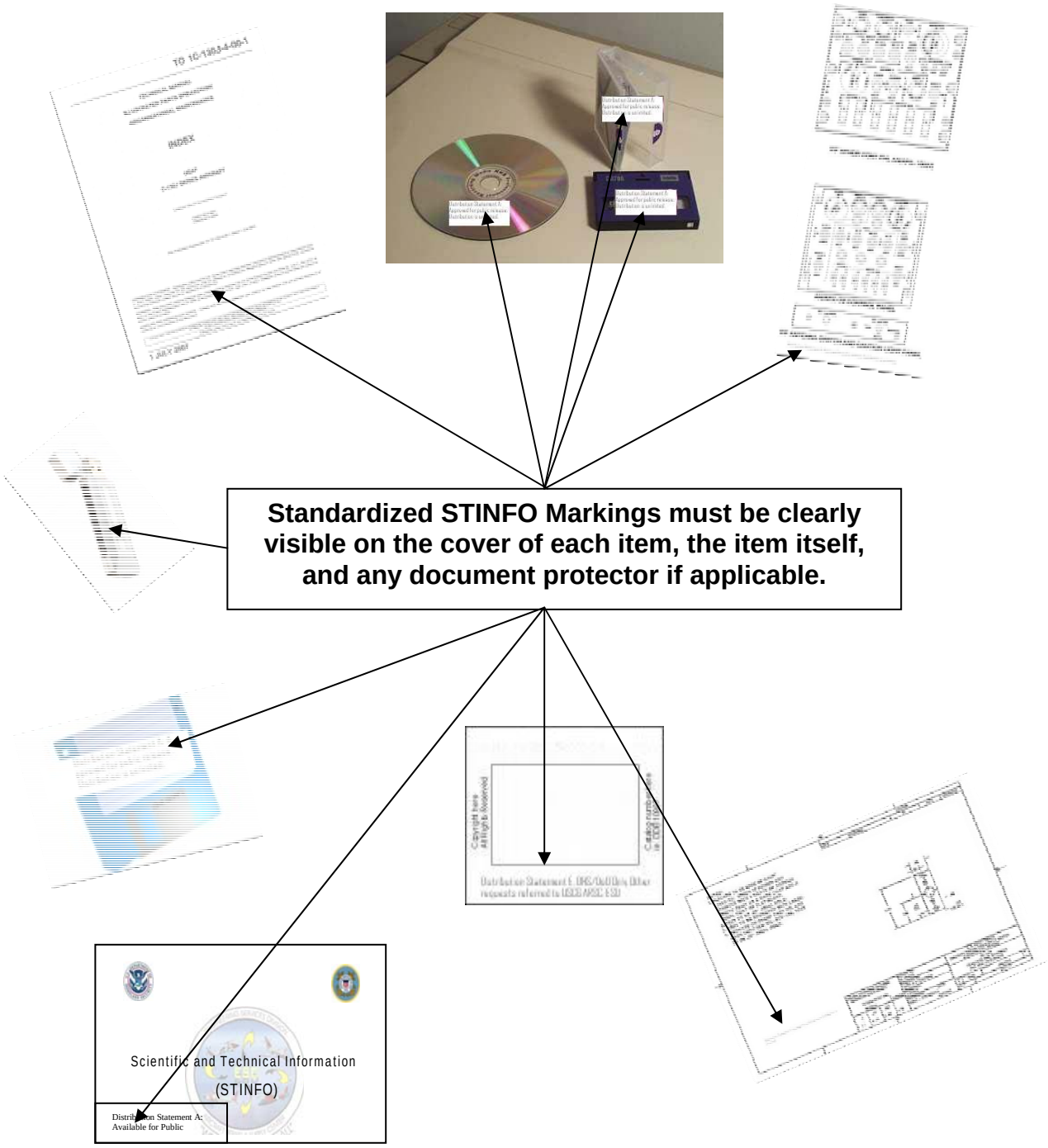
REFERENCES

Reference	Title
CGTO PG-85-00-290	Standardized STINFO Markings Process Guide
CGTO RG-95-00-100	A Quick Reference Guide For Marking DHS/CG/DoD Technical Documents
ADA 423966	Reference Guide for Marking DoD Documents
COMDTINST M5212.12 (series)	The Information and Life Cycle Management Manual
COMDTINST M5260.3 (series)	Coast Guard Freedom of Information (FOIA) and Privacy Acts (PA)
COMDTINST M5500.13 (series)	Automated Information Systems (AIS) Security Manual
COMDTINST M5510.23 (series)	Classified Information Management Program
DoD 5200.22M	National Industrial Security Program Operating Manual
DoD Instruction 5230.27	Presentation of DoD-Related Scientific and Technical Papers at Meetings
DoD Instruction 5230.29	Security and Policy Review of DoD Information for Public Release
DoD Regulation 5200-1-R	Information Security Program Regulation
DoD Directive 3200.12	DoD Scientific and Technical Information (STI) Program (STIP)
DoD Directive 5230.9	Clearance of DoD Information for Public Release
DoD Directive 5230.11	Disclosure of Classified Military Information to Foreign Governments and International Organizations
DoD Directive 5230.24	Distribution Statements on Technical Documents
DoD Directive 5230.25	Withholding of Unclassified Technical Data from Public Disclosure
DoD Directive 5400.7	DoD Freedom of Information Act (FOIA) Program
DoD Directive 5400.11	Department of Defense Privacy Program
DoD Directive 8910.1	Management and Control of Information Requirements
DFARS 252.27.4/252.227	Proprietary Information
DHS MD 11042.1	Safeguarding Sensitive But Unclassified (FOUO) Information
EO 12356	National Security Information
EO 12829	National Security Industrial Security Program (NISP)
EO 13292/12958	Classified National Security Information
Public Law 22 USC Sec: 2778, 2779, 2780, 2785, 2794	Title 11 – Foreign Relations and Intercourse, Chapter 39 – Arms Export Control, Subchapter 1 – Foreign and National Security Policy Objectives and Restraints
AFPD 61-2	Management of STINFO
AFI 61-201	Responsibilities of the STINFO Officer
AFI 61-202	Scientific Research and Development
AFI 61-204	Disseminating Scientific and Technical Information
PN 05-701	Air Force Eagle Look STINFO Study

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

PLACEMENT OF STANDARDIZED STINFO MARKINGS



Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

STANDARDIZED STINFO DISTRIBUTION STATEMENTS

Public Access/Unlimited	A	Distribution Statement A: Approved for public release; distribution is unlimited.
U.S. Government Agencies Only	B	Distribution Statement B: Distribution authorized to U.S. Government Agencies only (fill in reason) (date of determination). Other requests shall be referred to (insert Controlling CG/DoD Office).
U.S. Government Agencies and their Contractors	C	Distribution Statement C: Distribution authorized to U.S. Government Agencies and their contractors (fill in reason) (date of determination). Other requests shall be referred (insert Controlling CG/DoD Office).
DHS/CG/DoD/and their Contractors	D	Distribution Statement D: Distribution authorized to the DHS/CG/DoD and their contractors (fill in reason) (date of determination). Other requests shall be referred to (insert Controlling CG/DoD Office).
CG.DoD Only	E	Distribution Statement E: Distribution authorized to the CG/DoD only (fill in reason) (date of determination). Other requests shall be referred to (insert Controlling CG/DoD Office).
Further dissemination required from the controlling office (Originator)	F	Distribution Statement F. Further dissemination only as directed by (insert Controlling CG/DoD Office) (date of determination) or higher CG/DoD authority.
Agencies/Individuals Authorized to Receive Export Controlled Unclassified **** Do Not Use On CG Documents****	X	Distribution Statement X: Distribution authorized to U.S. Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with DoDD 5230.25 (date of determination). Controlling office is (insert Controlling CG/DoD Office).
Export-Control Warning		WARNING – This document contains technical data whose export is restricted by the Arms Export-Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C. App 2401, et. seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.
For Official Use Only (FOUO)		This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the FOIA. Exemption(s) _____ apply/applies.
Destruction Notice		DESTRUCTION NOTICE: For classified documents, follow the procedures in DoD 5200.22-M, National Industrial Security Program Operating Manual, Section 5-705 or DoD 5200.1-R, Information Security Program Regulation, Chapter VI, Section 7. For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

NOTE

Distribution Statement X will not be used on any CG STINFO. Any DoD STINFO that contains the Distribution X shall be handled as Export-Controlled.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

FULL EXPORT-CONTROL WARNING STATEMENT

NOTICE TO ACCOMPANY THE DISSEMINATION OF EXPORT-CONTROLLED TECHNICAL DATA

Export of the attached information which includes, in some circumstances, release to foreign nationals within the United States, without first obtaining approval or license from the Department of State for items controlled by the International Traffic in Arms Regulations (ITAR) or the Department of Commerce for controlled by the Export Administration Regulations (EAR), may constitute a violation of the law.

Under 22 U.S.C. 2778, the penalty for unlawful export of items or information controlled under the ITAR is up to 2 years imprisonment, or a fine of $100,000 or both. Under U.S.C., Appendix 2410, the penalty for unlawful export of items or information controlled under the EAR is a fine of up to $1,000,000, or five times the value of the exports, whichever is greater, or for an individual, imprisonment of up to 10 years, or a fine of up to $250,000, or both.

In accordance with your certification that establishes you as a “qualified U.S. contractor,” unauthorized dissemination of this information is prohibited and may result in your disqualification as a qualified U.S. contractor, and may be considered in determining your eligibility for future contract with the Department of Defense.

The U.S. Government assumes no liability for direct patent infringement, contributory patent infringement, or misuse of technical data.

The U.S. Government does not warrant the adequacy, accuracy, currency, or completeness of the technical data.

The U.S. Government assumes no liability for loss, damage, or injury, resulting from the manufacture or use for any purpose of any product, article, system, or material involving reliance upon any or all technical data furnished in response to the request for technical data.

If the technical data furnished by the Government will be used for commercial manufacturing or other profit potential, a license for such use may be necessary. Any payments made in support of the request for data do not include or involve any license rights.

A copy of this notice shall be provided with any partial or complete reproduction of these data that are provided to qualified U.S. contractors.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

Distribution Statement Matrix

		Who Can Have Access to the Information						
Coast Guard Security Level		III	II	II	II	II	I or II	II
10 Reasons for Imposing Distribution Statements Does the information refer to?		Public Access/ Unlimited	Gov't Agencies Only	Gov't Agencies and their Contractors	DHS/CG/DoD and their Contractors	DHS/CG/ DoD only	Distribute "Only" with Approval from Owner	***Agencies/ Individuals Authorized to Receive Unclassified Export-Controlled
		A	B	C	D	E	F	X
1	Foreign Government Information		●	●	●	●	●	
2	Proprietary Information		●			●	●	
3	Critical Technology		●	●	●	●	●	
4	Test and Evaluation		●			●	●	
5	Contractor Performance Evaluation		●			●	●	
6	Premature Dissemination		●			●	●	
7	Administrative/Operational Use		●	●	●	●	●	
8	Software Documentation		●	●	●	●	●	
9	Specific Authority: (Executive Orders, Federal Regs, Atomic Energy Act, or Stevenson-Wydler Act)		●	●	●	●	●	
10	Direct Military Support **Normally used on Classified STINFO**					●	●	

The information can be released to anyone	●						
Used on Classified Information but can be used on Unclassified when approved from the Controlling Office (Owner)						●	
Export-Control of Unclassified Technical Data Not used in DHS/CG							●

** Distribution Statement "X": It is CG/DoD policy that Distribution Statement X by itself does not accurately limit the distribution of the information to an audience and therefore will not be used on any CG document.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

TEN REASONS FOR DISTRIBUTION STATEMENT RESTRICTIONS

Foreign Government Information: This is information provided to the United States by, or information produced by the united States as a result of collaboration with, a foreign government or governments or an international organization of governments.
Proprietary Information: Information that is not owned by the U.S. Government, protected by a contractor's "limited rights" statement, or received with the understanding that it not be routinely transmitted outside of the U.S. Government.
Test and Evaluation: Protects commercial products or military hardware test and evaluation results when such disclosure may cause unfair advantage or disadvantage to the manufacturer of the product.
Contractor Performance Evaluation: Protects management-review information, contract-performance evaluation records, or other advisory documents evaluating contractors' programs.
Critical Technology: Protects technology consisting of arrays of design and manufacturing know-how, keystone manufacturing, inspection, and test equipment; keystone materials; or goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the United States. "Critical Technology" (also referred to as "military critical technology") is the terminology used by the DoD for export-controlled items.
Premature Dissemination: Protects systems or hardware information in the developmental or conceptual stage to prevent premature disclosure that might jeopardize the inventor's rights to obtain a patent.
Software Documentation: Protects software documentation and data releasable according to the software license terms.
Administrative/Operational Use: Protects technical or operational data or information from automatic dissemination under the international exchange program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical reports, and other publications containing valuable technical or operational data.
Specific Authority: Protects information not specifically included in the other authorized reasons, but which requires protection according to a valid governing authority, such as Executive Order, Atomic Energy Act or Stevenson-Wydler Act, or federal regulations.
Direct Military Support: Protects export-controlled, technical information of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize an important technological or operation military advantage for the U.S.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

DEPARTMENT OF HOMELAND SECURITY

NON-DISCLOSURE AGREEMENT

I, _____, an individual official, employee, consultant, or subcontractor of or to _____ (the Authorized Entity), intending to be legally bound, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of the United States Government.

(Signer will acknowledge the category or categories of information that he or she may have access to, and the signer's willingness to comply with the standards for protection by placing his or her initials in front of the applicable category or categories.)

Initials	**Protected Critical Infrastructure Information (PCII)**

I attest that I am familiar with, and I will comply with all requirements of the PCII program set out in the Critical Infrastructure Information Act of 2002 (CII Act) (Title II, Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296, 196 Stat. 2135, 6 USC 101 et seq.), as amended, the implementing regulations thereto (6 CFR Part 29), as amended, and the applicable PCII Procedures Manual, as amended, and with any such requirements that may be officially communicated to me by the PCII Program Manager or the PCII Program Manager's designee.

Initials	**Sensitive Security Information (SSI)**

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of SSI information as cited in this Agreement and in accordance with 49 CFR Part 1520, "Protection of Sensitive Security Information," "Policies and Procedures for Safeguarding and Control of SSI," as amended, and any supplementary guidance issued by an authorized official of the Department of Homeland Security.

Initials	**Other Sensitive but Unclassified (SBU)**

As used in this Agreement, sensitive but unclassified information is an over-arching term that covers any information, not otherwise indicated above, which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, as amended, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information categorized by DHS or other government agencies as: For Official Use Only (FOUO); Official Use Only (OUO); Sensitive Homeland Security Information (SHSI); Limited Official Use (LOU); Law Enforcement Sensitive (LES); Safeguarding Information (SGI); Unclassified Controlled Nuclear Information (UCNI); and any other identifier used by other government agencies to categorize information as sensitive but unclassified.

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of the information to which I am granted access as cited in this Agreement and in accordance with the guidance provided to me relative to the specific category of information.

I understand and agree to the following terms and conditions of my access to the information indicated above:

1. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of information to which I have been provided conditional access, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

2. By being granted conditional access to the information indicated above, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to the specific categories of information to which I am granted access.

3. I attest that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with the terms of this Agreement and the laws, regulations, and/or directives applicable to the specific categories of information to which I am granted access. I understand that the United States Government may conduct inspections, at any time or place, for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding information under this Agreement.

Downloaded from http://www.everyspec.com

4. I will not disclose or release any information provided to me pursuant to this Agreement without proper authority or authorization. Should situations arise that warrant the disclosure or release of such information I will do so only under approved circumstances and in accordance with the laws, regulations, or directives applicable to the specific categories of information. I will honor and comply with any and all dissemination restrictions cited or verbally relayed to me by the proper authority.

5. (a) For PCII - (1) Upon the completion of my engagement as an employee, consultant, or subcontractor under the contract, or the completion of my work on the PCII Program, whichever occurs first, I will surrender promptly to the PCII Program Manager or his designee, or to the appropriate PCII officer, PCII of any type whatsoever that is in my possession.
(2) If the Authorized Entity is a United States Government contractor performing services in support of the PCII Program, I will not request, obtain, maintain, or use PCII unless the PCII Program Manager or Program Manager's designee has first made in writing, with respect to the contractor, the certification as provided for in Section 29.8(c) of the implementing regulations to the CII Act, as amended.
(b) For SSI and SBU - I hereby agree that material which I have in my possession and containing information covered by this Agreement, will be handled and safeguarded in a manner that affords sufficient protection to prevent the unauthorized disclosure of or inadvertent access to such information, consistent with the laws, regulations, or directives applicable to the specific categories of information. I agree that I shall return all information to which I have had access or which is in my possession 1) upon demand by an authorized individual; and/or 2) upon the conclusion of my duties, association, or support to DHS; and/or 3) upon the determination that my official duties do not require further access to such information.

6. I hereby agree that I will not alter or remove markings, which indicate a category of information or require specific handling instructions, from any material I may come in contact with, in the case of SSI or SBU, unless such alteration or removal is consistent with the requirements set forth in the laws, regulations, or directives applicable to the specific category of information or, in the case of PCII, unless such alteration or removal is authorized by the PCII Program Manager or the PCII Program Manager's designee. I agree that if I use information from a sensitive document or other medium, I will carry forward any markings or other required restrictions to derivative products, and will protect them in the same matter as the original.

7. I hereby agree that I shall promptly report to the appropriate official, in accordance with the guidance issued for the applicable category of information, any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation, I have knowledge of and whether or not I am personally involved. I also understand that my anonymity will be kept to the extent possible when reporting security violations.

8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to the information covered by this Agreement. This may serve as a basis for denying me conditional access to other types of information, to include classified national security information.

9. (a) With respect to SSI and SBU, I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of the information not consistent with the terms of this Agreement.
(b) With respect to PCII I hereby assign to the entity owning the PCII and the United States Government, all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of PCII not consistent with the terms of this Agreement.

10. This Agreement is made and intended for the benefit of the United States Government and may be enforced by the United States Government or the Authorized Entity. By granting me conditional access to information in this context, the United States Government and, with respect to PCII, the Authorized Entity, may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I understand that if I violate the terms and conditions of this Agreement, I could be subjected to administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations, or directives applicable to the category of information involved and neither the United States Government nor the Authorized Entity have waived any statutory or common law evidentiary privileges or protections that they may assert in any administrative or court proceeding to protect any sensitive information to which I have been given conditional access under the terms of this Agreement.

Downloaded from http://www.everyspec.com

11. Unless and until I am released in writing by an authorized representative of the Department of Homeland Security (if permissible for the particular category of information), I understand that all conditions and obligations imposed upon me by this Agreement apply during the time that I am granted conditional access, and at all times thereafter.

12. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

13. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or non-disclosure Agreement which I have executed or may execute with the United States Government or any of its departments or agencies.

14. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958, as amended; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

15. Signing this Agreement does not bar disclosures to Congress or to an authorized official of an executive agency or the Department of Justice that are essential to reporting a substantial violation of law.

16. I represent and warrant that I have the authority to enter into this Agreement.

17. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me any laws, regulations, or directives referenced in this document so that I may read them at this time, if I so choose.

DEPARTMENT OF HOMELAND SECURITY

NON-DISCLOSURE AGREEMENT

Acknowledgement

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

I make this Agreement in good faith, without mental reservation or purpose of evasion.

Signature:

WITNESS:

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

Signature:

This form is not subject to the requirements of P.L. 104-13, “Paperwork Reduction Act of 1995” 44 USC, Chapter 35.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

EXAMPLE OF
UNIT LEVEL STINFO REVIEWER DESIGNATION LETTER

U.S. Department of Homeland Security
United States Coast Guard

CommandING Officer
United States Coast Guard
Aviation Logistics Center

1664 Weeksville Road
Elizabeth City NC 27909-500
Staff Symbol: esd
Phone: (252) 335-6240
Fax: (252) 335-6463
Email: susan.m.webb@uscg.mil

5260

MEMORANDUM

From: E.J.GIBBONS, CAPT
CG ALC

Reply to Attn of: esd-tech pubs
STINFO Manager
(252) 335-6829

To: JOE COASTIE
Thru: CG ALC (Division Chief)

Subj: LETTER OF DESIGNATION AS (Unit Name) STINFO REVIEWER

Ref:
(a) Management of Scientific and Technical Information (STINFO), COMDTINST M5260.4 (series)
(b) Executive Orders (EO): 12356, 12829, 13292/12958
(c) U.S. Code 22 USC Sec. 2778, 2779, 2780, and 2794
(d) Standardized STINFO Markings Process Guide, CGTO PG-85-00-290
(e) DoD 5200.22M, National Industrial Security Program Operating Manual

1. In accordance with reference (a), you are designated as the (Unit Name) STINFO Reviewer. Your responsibilities include ensuring that all technical data, technical documents and technical information as defined in references (a) and (d) are marked with the predetermined Standardized STINFO Markings prior to distribution beyond the originator of the information.

2. Your designation may not be delegated. The designation of the (Unit Name) STINFO Reviewer will be documented within your training file.

3. The (Unit Name) is committed to maintaining the security of Unclassified Limited-Access STINFO in accordance with references (b) and (c). This is accomplished by the assignment of the Standardized STINFO Markings by the originator of the technical information which includes a Distribution Statement, Export-Control Warning Statement (if applicable), Destruction Notice and Intellectual Property Notice (if applicable).

#