U.S. Department of Homeland Security

United States Coast Guard

MANAGEMENT OF SCIENTIFIC AND TECHNICAL INFORMATION (STINFO)

COMDTINST M5260.6A

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

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

Commandant
United States Coast Guard

Stop 7714
2703 Martin Luther King Jr. Ave SE
Washington DC 20593-7714
Staff Symbol: CG-444
Phone: 202 475-5645

COMDTINST M5260.6A

16 SEPT 2015

COMMANDANT INSTRUCTION M5260.6A

Subj: MANAGEMENT OF SCIENTIFIC AND TECHNICAL INFORMATION (STINFO)

Ref: (a) Safeguarding Sensitive but Unclassified (For Official Use Only) Information, Department of Homeland Security Management Directives MD Number 11042.1
(b) Security Information (SSI), Department of Homeland Security Management Directives System MD Number 11056.1, Sensitive
(c) Executive Order 13526, Classified National Security Information

1. PURPOSE. This Manual prescribes the policies and procedures and assigns responsibilities for the United States Coast Guard (USCG) Scientific and Technical Information (STINFO) Program. The purpose of the Manual is to establish a standardized program for USCG personnel and those under binding, legal agreement to the Department of Homeland Security (DHS), who use, originate, review, or assign distribution statements, export-control warnings, intellectual property statements or destruction notices (STINFO Markings) to information containing STINFO.

2. ACTION. All USCG unit commanders, Commanding Officers, Officers-in-Charge, Deputy/Assistant Commandants, Chiefs of Headquarters staff elements, USCG Reserve, and USCG Auxiliary personnel, and other individuals or organizations as required by binding agreement or obligation with the USCG and the DHS will comply with the provisions of this Instruction. Internet release is authorized.

3. DIRECTIVES AFFECTED. Management of Scientific and Technical Information (STINFO), COMDTINST M5260.6 is cancelled.

4. DISCUSSION. Identifying and applying the correct STINFO Markings to all required documents or information is essential to preclude the agency, service, or customer from significant liability and possibly affecting the national security of the country. STINFO includes all types of technical data in numerous formats including draft, working, hard copy, digital, and electronic documents. It includes information that relates to military operations and systems including research, development,

DISTRIBUTION– SDL No. 166

	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	X				X								X		X	X			X							
B																										
C																										
D																							X			
E																										
F																										
G																										
H																										

NON-STANDARD DISTRIBUTION:

engineering, testing, evaluation, production, logistics and operations. STINFO can be any information that is used to design, procure, support, maintain, repair or overhaul products, services, or equipment. 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. Governing references are cited in Appendix A. DoD references are included and applicable due to USCG-Joint Service interoperability requirements. It is important to note that the withholding of information subject to release under the Freedom of Information Act (FOIA) and Privacy Acts may result in severe penalties and consequences.

5. DISCLAIMER. This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is intended to provide operational guidance for USCG personnel and is not intended to nor does it impose legally-binding requirements on any party outside the USCG.

6. MAJOR CHANGES.

   a. The USCG STINFO program management is changed from the Aviation Logistics Center (ALC) Engineering Services Division (ESD) to the Configuration Management Division (CG-444).

   b. All USCG Logistics Centers (i.e., Aviation Logistics Center (ALC), Shore Infrastructure Logistics Center (SILC), and Surface Forces Logistics Center (SFLC)) and the Command, Control, Communications, Computers, and Information Technology Service Center (C4ITSC) (Collectively referred to as LC/C4ITSC) will designate in writing a STINFO Manager (SM) and an alternate to serve as the single authoritative point of contact for all scientific and technical information matters, reviews, and approvals.

   c. Paragraph 3.B.7 added responsibilities for the Unit Level STINFO Reviewer.

   d. Export Control is no longer a Distribution Statement. It is a reason that can be used with Distribution Statements B, C, D, or E. Distribution X is no longer used; Direct Military Support is used with Distribution E only.

   e. There are two new reasons that may be used with Distribution Statements: Operations Security that is used with Distribution Statements B and E only and Vulnerability Information which is used with Distribution Statements B, C, D, or E.

   f. Appendix A has updated DHS and DoD reference information. New references for the Export Administration Regulations and U.S. Munitions List (USML) are added.

   g. Appendix B, Acronyms and Terms is added.

   h. Enclosure 4, a USCG STINFO marking process map is added.

7. IMPACT ASSESSMENT. The major changes introduced in this update assigning the STINFO program management to Commandant (CG-444) and for the LC/C4ITC to have a STINFO manager were reviewed and found to have no additional impact on current funding and staffing levels. The requirements for marking, handling, distribution, storage, and disposal of STINFO material have not changed.

8. ENVIRONMENTAL ASPECTS AND IMPACT CONSIDERATIONS.

   a. The development of this Manual and the general policies contained within it have been thoroughly reviewed by the originating office in conjunction with the Office of Environmental Management, and are categorically excluded (CE) under current USCG CE #33 from further environmental analysis, in accordance with Chapter 2.B.2 and Figure 2-1 of the National Environmental Policy Act (NEPA) Implementing Procedures and Policy for Considering Environmental Impacts, COMDTINST M16475.1 (series). Because this Manual implements, without substantive change, the applicable Commandant Instruction or other federal agency regulations, procedures, manuals, and other guidance documents, USCG categorical exclusion #33 is appropriate.

   b. This directive will not have any of the following: significant cumulative impacts on the human environment; substantial controversy or substantial change to existing environmental conditions; or inconsistencies with any Federal, State, or local laws or administrative determinations relating to the environment. All future specific actions resulting from the general policies in this Instruction must be individually evaluated for compliance with the NEPA, Council on Environmental Policy NEPA regulations at 40 CFR Parts 1500-1508, Department of DHS and USCG NEPA policy, and compliance with all other environmental mandates.

9. DISTRIBUTION. No paper distribution will be made of this Manual. An electronic version will be located on the following Commandant (CG-612) web sites. Internet: http://www.uscg.mil/directives/ and CGPortal: https://cgportal2.uscg.mil/library/directives/SitePages/Home.aspx.

10. RECORDS MANAGEMENT CONSIDERATIONS. This Manual has been evaluated for potential records management impacts. The development of this Manual has been thoroughly reviewed during the directives clearance process, and it has been determined there are no further records scheduling requirements, in accordance with Federal Records Act, 44 United States Code (U.S.C.) §3101 et seq., National Archives and Records Administration (NARA) requirements, and the Information and Life Cycle Management Manual, COMDTINST M5212.12 (series).

11. FORMS/REPORTS. The forms referenced in this Manual are available in USCG Electronic Forms on the Standard Workstation or on the Internet.

12. REQUESTS FOR CHANGES. Recommendations for changes and improvements to this Manual will be submitted via the chain of command to the CM Division, Commandant (CG-444) using Publication Change Recommendation, Form CG-22.

B. D. BAFFER /s/
Rear Admiral, U. S. Coast Guard
Assistant Commandant for Engineering and Logistics

TABLE OF CONTENTS

INTENTIONALLY LEFT BLANK

CHAPTER 1. OVERVIEW

A. General. Scientific and Technical Information (STINFO) is defined as any recorded information, regardless of its physical form or characteristics that contains scientific and technical information, or technical data including production, engineering, and logistics information including:

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

B. Manual Guidelines. This Manual addresses important security and standardization issues of which the end-user, originator, developer, or publisher of information requiring a limited distribution or access needs to be cognizant. Chapter 2 and the subsequent chapters of this instruction provide an overview of the STINFO program and the necessary actions required when utilizing this information. This Manual provides the knowledge required for the management of and the assignment of the STINFO Markings for unclassified limited-access information to the Logistics Center (LC)/Service Center (SC) STINFO Manager, Unit FOIA Officer, Unit Level STINFO Reviewer, originator, developer, or publisher of STINFO.

C. STINFO Authority. The overarching authority of the USCG STINFO program is the Assistant Commandant for Engineering and Logistics, Commandant (CG-4). The Configuration Management Division, Commandant (CG-444) is the STINFO Program Manager and manages the program.

D. STINFO Manager. All USCG LCs (SFLC, ALC, and the SILC), the Research and Development Center, and the C4IT Service Center will designate a STINFO Manager (SM) in writing and an alternate to serve as the single, authoritative point of contact for all scientific and technical information matters, reviews, or approvals. The SM will:

1. Comply with the provisions of this Manual.
2. Comply with the requirements of the USCG STINFO policy and ensure scientific, technical, and engineering information is properly created, documented, controlled, marked, disseminated, and disposed.
3. Ensure personnel are trained and educated in the management of STINFO to provide a basic understanding of marking and distribution statements. New employee training and refresher training requirements also apply.

E. Responsibility. All USCG commanding officers, officers-in-charge, deputy/assistant commandants, chiefs of headquarters staff elements, USCG Reserve, and USCG Auxiliary (Controlling Office) or the designated representative (Example: FOIA Officer, PAO, Unit STINFO Reviewer) responsible for the origination of a technical document have the overall responsibility for assuring that required reviews are completed and the appropriate STINFO Markings are assigned. They will:

1. Comply with the provisions of this Manual.

2. Comply with the requirements of the USCG STINFO policy to ensure scientific and technical information is properly created, documented, controlled, disseminated, or disposed. Designate a scientific and technical information manager/reviewer.
3. Ensure personnel are trained and educated in the management of STINFO to provide a basic understanding of marking and distribution statements. New employee training and refresher training requirements also apply.

CHAPTER 2. STINFO USER REQUIREMETS

A. General.

1. End User. The key word for all end-users of STINFO is **AWARENESS**. All STINFO will be labeled 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, drawings, papers, reports). The information may also be located on electronic storage devices (CD, DVD, portable hard drives, etc.) and their protective covers, as well as on the first slide of an electronic presentation or briefing (see Enclosure (1)).

2. STINFO Classification. STINFO can be categorized with a Security Classification (Top Secret, Secret, or Confidential) Reference: Classified Information Management Program, COMDTINST M5510.23 (series) as explained in paragraph 3.C.1. STINFO may also be categorized as unclassified but having a limited-access, or unclassified and available to the public.

3. Markings. All unclassified and unclassified limited-access STINFO not protected by the FOIA or Privacy Acts (PA), or listed as an exception in this chapter, requires the STINFO Markings which consist of a Distribution Statement, Export-Control Warning Statement (if applicable) and a Destruction Notice. Standardized STINFO Marking Process Guide, CGTO PG-85-00-290-A, Chapter 6, has examples of sample STINFO markings. The Standardized STINFO Marking Process Guide is located on the Technical Manual Applications System (TMAPS) web site at: https://mynatec.navair.navy.mil/. TMAPS can also be accessed from the Coast Guard Applications page located on the USCG Portal. You must register for a user account to access TMAPS. STINFO should also be marked with an Intellectual Property (Proprietary Information) Notice (if applicable). See Enclosure (1), Enclosure (2), and Chapter 4.

   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 responsible 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 USML, Code of Federal Regulations (CFR) Title 22, Part 121.15 (a) (1), specifically states that any information pertaining to USCG surface vessels as well as any aircraft used by the military may not be unlawfully exported. Individuals should exercise extreme caution to ensure that they are not unintentionally exporting limited-access STINFO as the definition of exporting can be confusing (see 22 U.S.C. Sec. 2794). Allowing this information to be obtained by the wrong person(s) can result in serious fines and penalties for an individual 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. 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) either printed on the cover page or included as an attachment. Here are examples that can be interpreted as exporting information:

(1) The topic of a briefing or presentation that 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) or a USCG IT System.

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

(5) Communicating (Telephone, Cellular Phone, Instant Messaging, Text Message, Tweeting, etc…) limited-access information to unauthorized individuals.

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, Compact disk (CDs), Digital Video Disk (DVDs), or recorded media and 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.3.b, and thereby in violation of Public Laws and Executive Orders.

d. Disposal. 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 example of the actual destruction notice. **Proprietary STINFO must be shredded**. The destruction methods described below may only be used with DHS/USCG/DoD unclassified limited-access STINFO when 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.

(4) Documents approved for public release may be placed in recycle or regular trash receptacles as a whole document.

(5) Destroy classified documents in accordance with Information Security Program, DoD 5200.1-R.

(6) Destruction of Digital Media. Media containing unlimited distribution data may be recycled as is. Media containing unclassified, limited distribution data must be "cleared" before recycling: memory devices or hard drives must be reformatted and magnetic tapes must be erased.

e. Intellectual Property (IP) (Proprietary Information) Notice (if applicable). Owners of IP STINFO will negotiate with the 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.

(1) 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/USCG/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.

(2) 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 USCG/DoD publication.

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

f. Legacy. Any legacy STINFO received without the STINFO Markings with a publication date prior to the date of this Manual will be handled as if being marked with a Distribution Statement D (USCG/DoD and their contractors). Most new documents received without the STINFO Markings are done so inadvertently due to oversight or without the knowledge that the markings are required. The new STINFO will be returned to the originator in order to assign the STINFO Markings prior to any further distribution.

4. Exceptions to the STINFO Marking Rule. Certain documents do not require the STINFO Markings including:
   a. Technical proposals or similar documents submitted by contractors seeking USCG funds or contracts.
   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 USCG/DoD that have not been produced by or for the USCG/DoD such as a book of industry standards or a privately published scientific journal.
   d. Approved standard forms (USCG, 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 CG-444 STINFO PM, LC/C4ITSC STINFO managers, unit FOIA, Public Affairs Officer (PAO), Security Officer, Unit STINFO Reviewer, and the Originator. The STINFO PM can be found on the CG-444 Portal page under Contacts.
   2. The following chapters and Appendix A contain more in-depth information on the management and application of the USCG STINFO policy.

CHAPTER 3. ORIGINATOR, DEVELOPER, AND PUBLISHER OF STINFO

A. STINFO Marking Authority.

1. The STINFO PM is the managing authority for the USCG STINFO Program; ensuring standardization, oversight, and implementation of the STINFO Markings. See Enclosure (1).
2. USCG LC/C4ITSC STINFO managers will ensure that all scientific and technical information is properly managed and contains the applicable STINFO Markings. Enclosure (4) is a STINFO marking process map.

B. Responsibilities.

1. Unit Commanding Officer (Controlling Office). The Unit Commanding Officer or the designated representative (Example: FOIA Officer, PAO, Unit STINFO Reviewer) responsible for the origination of the technical document has the overall responsibility for assuring that required reviews are completed and the appropriate STINFO Markings are assigned.
2. Originator. Any originator who believes STINFO is not covered in an existing Security Classification Guide should be classified (Top Secret, Secret, Confidential) will 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. The Commandant, Deputy Commandant for Operations (DCO), and Assistant Commandant for Intelligence and Criminal Investigations, Commandant (CG-2) are the only three entities within the USCG allowed to classify a document with a Security Classification. For unclassified limited-access material, the originator should refer to the STINFO Markings Process Guide, CGTO PG-85-00-290 on FORCECOM's portal, or request assistance from the unit FOIA Officer 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 (5) and Enclosure (6)). The unit FOIA Officer 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 STINFO Markings are applied or reapplied, there is a reasonable possibility the information can be protected from unauthorized disclosure. For STINFO that is related to major weapon systems and may be subject to ITAR restrictions, originators will contact Commandant (CG-2) to adjudicate whether STINFO is suitable for distribution under ITAR.
3. Technical Writer or Graphics Illustrator/Technical Draftsperson. These individuals are responsible for the actual placement of the predetermined 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.

4. Contracting Officer's Representative (COR)/Project Manager (if applicable). The COR/Project Manager ensures the project results are documented and reviewed, 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 forwarded to the ALC ESD Technical Publications Branch for dissemination. Questions related to non-aviation documents should be directed to the designated SM at the cognizant LC/C4ITSC.
5. Unit Security Officer. The unit security officer will review any document deemed to contain information that should be considered for a security classification (see Originator above).
6. Unit FOIA/PAO Officer. The FOIA Officer and PAO will assist other responsible entities (e.g., unit Operations or Intelligence Officers) by reviewing and approving all documents proposed for unlimited public release under Distribution Statement A.
7. Unit Level STINFO Reviewer. Every unit that may, or will produce, distribute, or present information containing copyrights, intellectual property (proprietary information), patents, trademarks, or Export-Controlled information will designate a Unit Level STINFO Reviewer who will oversee compliance with the USCG STINFO program at that unit.
8. STINFO Program Manager. The STINFO PM oversees the STINFO Program. Specific responsibilities include assisting LC/C4ITSC SM, unit FOIA Officers/PAO, and originators comply with STINFO policy, coordination of STINFO Awareness Training, and representing USCG interests at STINFO meetings and conferences. The STINFO PM will maintain a SECRET clearance.
9. STINFO Managers. LC/C4ITSC STINFO Managers will oversee execution of the USCG Program to the fleet, assist the unit-level STINFO reviewers and originators, and ensure STINFO policy compliance. They will maintain and annually update a record of designated unit-level STINFO reviewers and are responsible for the actual markings (process) training.

C. Mandatory Markings on STINFO. All STINFO will 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 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 STINFO Markings when the document or item is reviewed, requested, or updated. Any unmarked legacy STINFO which requires any restrictions in distribution can only be released to USCG/DoD personnel or their contractors after it is reviewed and properly marked. Unmarked new STINFO will be returned to the originator in order to assign the STINFO Markings prior to any further distribution. All STINFO Markings will be made as depicted in Enclosure (1) and Enclosure (2). Exceptions to the marking rule are listed in Chapter 2.A.4. The five considerations of the STINFO Markings are listed below:

1. STINFO 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 M5510.23 (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 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 Acts, or is categorized as Export-Controlled by the Export Administration Act (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 who (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 will be used on all USCG/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. 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 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 (5) and Enclosure (6);

   c. Identity of the Controlling USCG/DoD Office/Originator (Owner);

   d. Date of review or determination for the limited-access.

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 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. The Export-Control Warning Statement is required on all STINFO referenced in the CCL or USML. As an example, the current USML states that all technical information applicable to USCG 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. The EAR/CCL website is at: http://www.access.gpo.gov/bis/ear/ear_data.html. The ITAR/USML website is at: http://www.access.gpo.gov/nara/cfr/waisidx_99/22cfr121_99.html.

4. Intellectual Property (IP) Notice. A contractor-placed notice specifies 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 and Commandant (CG-934) will ensure each individual contracted by the USCG to perform work, as well as the contracted corporation, is required to sign a Non-Disclosure Agreement, DHS Form 11000-6) (Enclosure (7)) prior to starting work in accordance with Reference (a).

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.3.d, for more in-depth information on the approved destruction methods for unclassified limited-access STINFO.

D. Freedom of Information Act (FOIA) and Privacy Acts (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 USCG records from other Federal agencies are not considered FOIA requests and are not 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 Coast Guard Freedom of Information (FOIA) and Privacy Acts 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. Prior to limiting or denying access to any requested information under FOIA, the FOIA Officer of the local command will consult with the applicable LC/C4ITSC Command FOIA and USCG Headquarters, Commandant (CG-0944) Legal as the final approval authority.

E. Automated Information System (AIS). Classified and unclassified but limited-access information handled by existing USCG Information Technology (IT) automated systems (CGLIMS, TIMOS, ALMIS, ATIMS, JEDMICS, CGTIMS, NETIMS, etc.) or any developing or future automated USCG IT systems or associated telecommunications will 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. DHS/CG/DoD and other government departments or agencies are subject to the AIS security requirements of that department or agency. Electronic mail containing STINFO will include the appropriate distribution statement in the subject line.

INTENTIONALLY LEFT BLANK

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 (STINFO Markings).

B. Authorized Access To STINFO. References (a), (b), and (c) control access to classified and unclassified information.

1. Classified Information (Top Secret, Secret, Confidential) and FOUO. 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 Members. May have access to unclassified information with Distribution Codes A, B, C, D, and E. 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, and E. Access to Distribution Code F may only be authorized with prior approval from the Controlling Office or Originator of the information.

4. DHS/USCG/DoD Contractors. The contracting officer will be responsible for ensuring that each contractor understands and signs a non-disclosure agreement prior to starting work. Those U.S. contractors currently holding grants or contracts with the DHS/USCG/DoD if permitted in their contract or grant or those contractors declared eligible for services by a sponsoring DHS/USCG/DoD activity on the basis of participation in a DHS/USCG/DoD Potential Contractor Program may have access to all unclassified Distribution Code A, C, and D information after signing a Non-Disclosure Agreement, DHS Form 11000-6, (Enclosure (7)).

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 immediately reported to the unit Security Officer.

2. Suspicious or inappropriate requests for information by any means, e.g., e-mail or verbal, will 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.

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.

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 DoD Scientific and Technical Information Program (STIP), DoDI 3200.12. The project COR will submit the final report to DTIC with an original Report Documentation Page, SF-298 (http://www.dtic.mil/) and to the applicable LC/C4ITSC STINFO Manager.

2. All STINFO received by the government in response to a contract award must be properly handled and marked with the STINFO Markings (Enclosure (2)). It is the responsibility of the originator to ensure the document is properly marked prior to delivery to the government.

B. Training. All USCG military, government, and contractor personnel will 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 USCG specific PowerPoint presentations. Future awareness training will be available via the USCG Learning Portal after development. The STINFO Program Manager is responsible for program familiarization training and the STINFO Managers are responsible for the actual marking training.

C. Forms/Reports. Applicable training records and designation of authority letters will be maintained at the unit level of military and civil service employees. Enclosure (8) is a sample designation letter. Contractor training records will be maintained by the respective contractor.

INTENTIONALLY LEFT BLANK

ADDITIONAL INFORMATION SOURCES

Information Source	Title
CGTO PG-85-00-290	STINFO Markings Process Guide (can be accessed from TMAPS on the Applications page on the CG Portal.)
DTIC 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 5220.22M	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 Manual 5200.01-V1-V4	DoD Information Security Program Manual
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 Instruction 3200.20	Scientific and Engineering Integrity
DoD Instruction 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
DHS MD 11056.1	Sensitive Security Information (SSI)
DHS MD 0460.1	Freedom of Information Act Compliance (FOIA)

EO 12356	National Security Information
EO 12829	National Security Industrial Security Program (NISP)
EO 13292/12958	Classified National Security Information
22 USC Sec: 2751, 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
Federal Records Act	Management of Federal Records
Export Administration Regulations (EAR) Part 774	Commerce Control List
CFR Title 32, Part 290	Defense Contract Audit Agency (DCAA) Freedom of Information Act Program [32 CFR 290]
CFR Title 22, Part 121	U.S. Munitions List (USML)
CFR Title 40, Parts 1500-1508	Protection of the Environment
Public Law 90-629, “Arms Export Control Act” as amended (22 U.S.C. 2751 et seq.)	Arms Export Control Act
42 U.S.C. Section 6602	National Science, Engineering, and Technology Policy and Priorities
22 U.S.C. Section 2794	Definitions
44 U.S.C. Section 3101	Records management by agency heads; general duties

ACRONYMS AND TERMS

AIS	Automated Information System
AECA	Arms Export-Control Act
CCL	Commerce Control List
COR	Contracting Officer's Representative
DTIC	Defense Technical Information Center
EAA	Export Administration Act
EAR	Export Administration Regulations
FOIA	Freedom of Information Act
FOUO	For Official Use Only
IP	Intellectual Property
ITAR	International Traffic in Arms Regulations
LC	Logistics Center
NDA	Non-Disclosure Agreement
NSA	National Security Agency
NSI	National Security Information
OCA	Original Classification Authority
PA	Privacy Acts
PAO	Public Affairs Officer
PCII	Protected Critical Infrastructure Information
SBU	Sensitive But Unclassified
SC	Service Center
SSI	Sensitive Security Information
STINFO	Scientific and Technical Information
USML	U.S. Munitions List

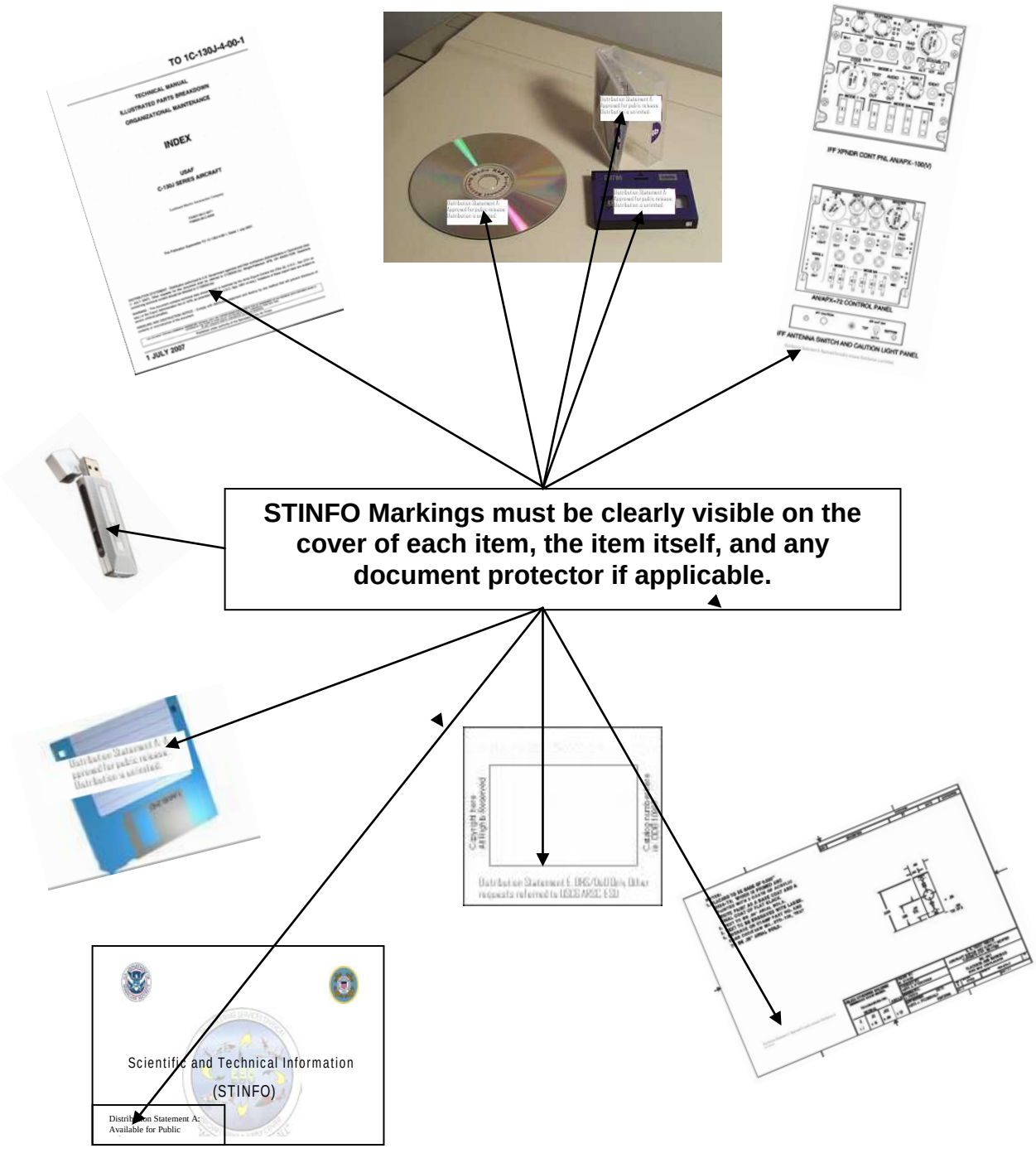
Terms:

1. Distribution Statement. Identifies who or what audience is authorized to view and or use the information. Distribution Statements must be applied to all Classified and Unclassified Limited-Access/Controlled Unclassified Information (CUI).

2. Technical Data. Technical Data is recorded information related to experimental, developmental, or engineering works that can be used to define engineering or manufacturing processes or to design, procure, support, maintain, operate, repair, or overhaul material. The data may be graphic or pictorial delineations in media such as drawings, illustrations, or photographs, text in specifications, or related performance, design type documents, or computer printouts.

3. Technical Information. Technical Information is any information, including scientific information that relates to research, development, engineering, test evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment.

PLACEMENT OF STINFO MARKINGS



INTENTIONALLY LEFT BLANK

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 will be referred to (insert Controlling USCG/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 will be referred (insert Controlling USCG/DoD Office).
DHS/USCG/DoD/and their Contractors	D	Distribution Statement D: Distribution authorized to the DHS/USCG/DoD and their contractors (fill in reason) (date of determination). Other requests will be referred to (insert Controlling USCG/DoD Office).
USCG/DoD Only	E	Distribution Statement E: Distribution authorized to the USCG/DoD only (fill in reason) (date of determination). Other requests will be referred to (insert Controlling USCG/DoD Office).
Further dissemination required from the controlling office (Originator)	F	Distribution Statement F. Further dissemination only as directed by (insert Controlling USCG/DoD Office) (date of determination) or higher USCG/DoD authority.
Export-Control Warning Statement		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 is no longer used; Direct Military Support is used with Distribution “E” only. Any DoD STINFO that contains the Distribution X will be handled as Export-Controlled.

INTENTIONALLY LEFT BLANK

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 20 years imprisonment, or a fine of $1,000,000 or both. Under 50 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.

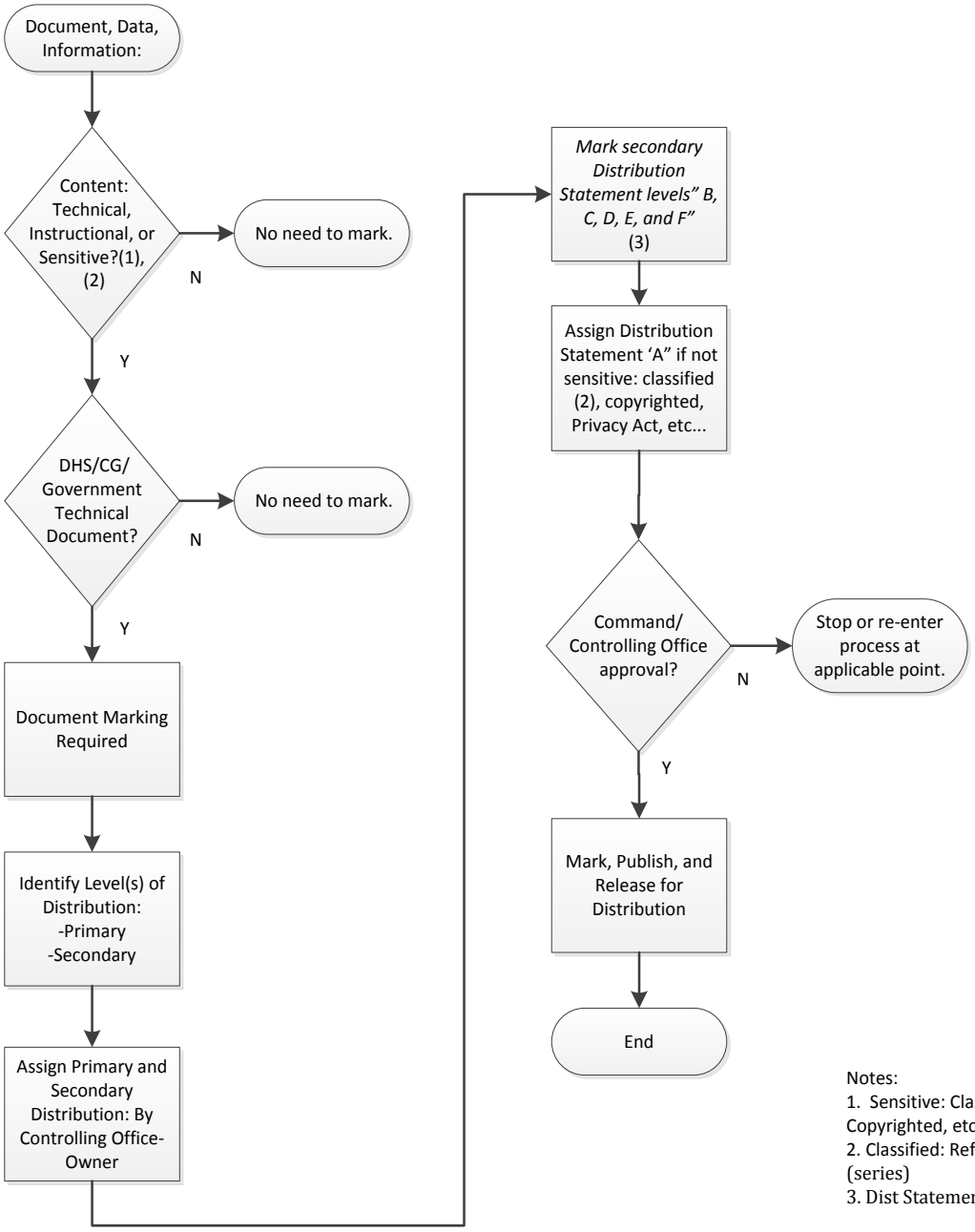
If the technical data furnished by the Government will be used for commercial manufacturing or other profit potential, a license for such use may be necessary. Any payments made in support of the request for data do not include or involve any license rights.

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

*Reference: DoDD 5230.25, Withholding of Unclassified Technical Data from Public Disclosure

INTENTIONALLY LEFT BLANK

STINFO MARKING PROCESS MAP



Notes:
1. Sensitive: Classified, Privacy Act, FOIA, Copyrighted, etc…
2. Classified: Ref:COMDTINST M5510.23 (series)
3. Dist Statement Level X is no longer used.

INTENTIONALLY LEFT BLANK

Distribution Statement Matrix						
* **Reasons for Designating Audiences for Secondary Distribution**	**CG/DoD Distribution Statement Levels/Codes**					
	A	**B**	**C**	**D**	**E**	**F**
APPROVED FOR PUBLIC RELEASE: *The information is approved for public release and does not contain controlled data.*	**X**					
FOREIGN GOVERNMENT INFORMATION: *The foreign government information furnished to the DHS/CG/DoD is restricted in its distribution.*						
DHS/CG/DoD components only					**X**	
U.S. Government Agencies only		**X**				
DHS/CG/DoD components and their contractors				**X**		
U.S. Government Agencies and their contractors			**X**			
Recipients as directed by the DHS/CG/DoD Controlling Office or higher DHS/CG/DoD Authority.						**X**
*Audience is the group of persons approved to receive the information.						

NOTE

Ensure the government negotiated rights statement is annotated on the cover sheet of the document if Proprietary Information is the reason for limiting access to the data, after the Export-Control Warning Statement and before the Destruction Notice.

*Reasons for Designating Audiences for Secondary Distribution	CG/DoD Distribution Statement Levels/Codes					
	A	B	C	D	E	F
PROPRIETARY INFORMATION: *The information is (1) owned by a nongovernmental entity and (2) protected by a contractor's Limited Rights Statement (LRS) or other agreement. Therefore, dissemination is restricted to:*						
DHS/CG/DoD components only					**X**	
U.S. Government Agencies only		**X**				
Recipients as directed by the DHS/CG/DoD Controlling Office or higher DHS/CG/DoD Authority						**X**
TEST AND EVALUATION: *The information results from testing and evaluation of commercial products or military hardware produced by a nongovernmental entity.*						
Routine dissemination of such results outside DHS/CG/DoD could result in unfair advantage or disadvantage to the manufacturer or producer.					**X**	
Routine dissemination of such results outside the U.S. Government could result in unfair advantage or disadvantage to the manufacturer or producer.		**X**				
Recipients as directed by the DHS/CG/DoD Controlling Office or higher DHS/CG/DoD Authority.						**X**
CONTRACTOR PERFORMANCE EVALUATION: *The information derived from the management review of a program, contractor, performance records, or other advisory documents evaluating a contractor program.*						
Routine dissemination of such results outside DHS/CG/DoD could result in unfair advantage or disadvantage to the contractor.					**X**	
Routine dissemination of such results outside the U.S. Government could result in unfair advantage or disadvantage to the contractor.		**X**				
Recipients as directed by the DHS/CG/DoD Controlling Office or higher DHS/CG/DoD Authority.						**X**
CRITICAL TECHNOLOGY: *The technology or information is on the U.S. Munitions List or the Commerce Control List and release of the technology or information to other than the designated group (identified below) will have a negative impact on U.S. military activities or help potential adversaries overcome military deficiencies:*						
DHS/CG/DoD components only					**X**	
U.S. Government Agencies only		**X**				
DHS/CG/DoD components and their contractors, but only if the contractors are registered with the DHS/CG/DoD to receive export-controlled data.				**X**		
U.S. Government Agencies and their contractors, but only if the contractors are registered with the DHS/CG/DoD to receive export-controlled data.			**X**			

***Reasons for Designating Audiences for Secondary Distribution**	**CG/DoD Distribution Statement Levels/Codes**					
	A	**B**	**C**	**D**	**E**	**F**
Recipients as directed by the DHS/CG/DoD Controlling Office or higher DHS/CG/DoD Authority.						**X**
SOFTWARE DOCUMENTATION: *Software documentation will be distributed according to the terms of the software license, which may restrict distribution to:*						
DHS/CG/DoD components only					**X**	
U.S. Government Agencies only		**X**				
DHS/CG/DoD components and their contractors				**X**		
U.S. Government Agencies and their contractors		**X**				
Recipients as directed by the DHS/CG/DoD Controlling Office or higher DHS/CG/DoD Authority						**X**
PREMATURE DISSEMINATION: *The information relates to patentable military systems or processes in the developmental stage and:*						
Disclosure at this time, except at the discretion of the Controlling Office, would compromise DHS/CG/DoD's interest in protecting a patentable technology.						**X**
Disclosure at this time, except to U.S. Government Agencies, would compromise DHS/CG/DoD's interest in protecting a patentable technology.		**X**				
Disclosure at this time, except to DHS/CG/DoD components, would compromise DHS/CG/DoD's interest in protecting a patentable technology.					**X**	
ADMINISTRATIVE/OPERATIONAL USE: *This information describes administrative procedures/instructions/directives or operations with technical or operational content (such as equipment maintenance, command, tactical, or weapons operations manuals). Such information may be unclassified but is considered sensitive information, and its distribution should be limited to entities that need it for Government purposes or to conduct official*						
DHS/CG/DoD components only					**X**	
U.S. Government Agencies only		**X**				
DHS/CG/DoD components and their contractors				**X**		
U.S. Government Agencies and their contractors			**X**			
Recipients as directed by the DHS/CG/DoD Controlling Office or higher DHS/CG/DoD Authority						**X**
DHS/CG/DoD components and their contractors				X		
U.S. Government Agencies and their contractors			**X**			
*****Audience is the group of persons approved to receive the information**.**						

*Reasons for Designating Audiences for Secondary Distribution	CG/DoD Distribution Statement Levels/Codes					
	A	B	C	D	E	F
SPECIFIC AUTHORITY: *The specific authority (Executive Order, statutes such as the Atomic Energy or Stevenson-Wydler Acts, Federal Regulations, etc.) governing this information restricts its distribution to:*						
DHS/CG/DoD components only					**X**	
U.S. Government Agencies only		**X**				
Recipients as directed by the DHS/CG/DoD Controlling Office or higher DHS/CG/DoD Authority						**X**
DIRECT MILITARY SUPPORT: *The technical data is export-controlled and of such military signi fi cance to another country or to a joint U.S.-foreign program that its release for other than direct support of DHS/CG/DoD activities potentially jeopardizes an important military advantage of the U.S. Release can be made:*						
To any DHS/CG/DoD component in the joint program					**X**	
Recipients as directed by the DHS/CG/DoD Controlling Office ce or higher DHS/CG/DoD authority						**X**
EXPORT CONTROLLED: *To protect information subject to the provisions of International Traffic in Arms Regulations (ITAR)*		**X**	**X**	**X**	**X**	**X**
OPERATIONS SECURITY: *To protect information and technical data that may be observed by adversary intelligence systems and determining what indicators hostile intelligence systems may obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries*		**X**			**X**	**X**
VULNERABILITY INFORMATION: *To protect information and technical data that provides insight into vulnerabilities of U.S. critical infrastructure, including DoD warfi ghting infrastructure, vital to National Security that are otherwise not publicly available*		**X**	**X**	**X**	**X**	**X**
*Audience is the group of persons approved to receive the information.						

NOTE

Unmarked legacy STINFO will be handled as if marked with a Distribution Statement D: DHS/CG/DoD and their Contractors, as Export-Controlled, and destroy by any means that would prevent reconstruction.

KEY 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.
Operations Security: To protect information and technical data that may be observed by adversary intelligence systems and determining what indicators hostile intelligence systems may obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries**.**

Vulnerability Information: To protect information and technical data that provides insight into vulnerabilities of U.S. critical infrastructure, including DoD warfighting infrastructure, vital to National Security that are otherwise not publicly available.

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, 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.

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 will return all information to which I have had access or which is in my possession 1) upon demand by an authorized individual; or 2) upon the conclusion of my duties, association, or support to DHS; 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 will 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.

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 will remain in full force and effect.

13. My execution of this Agreement will 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.

INTENTIONALLY LEFT BLANK

EXAMPLE OF
LC/C4ITSC/UNIT LEVEL STINFO MANAGER/REVIEWER DESIGNATION LETTER

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

Address:

Staff Symbol:
Phone: (
Fax:
Email:

5260

MEMORANDUM

From: TBD, CAPT
USCG LC/C4ITSC/Unit

Reply to TBD
Attn of: TBD

To: TBD

Subj: LETTER OF DESIGNATION AS LC/C4ITSC/Unit (Insert Name) STINFO MANAGER/REVIEWER

Ref: (a) Management of Scientific and Technical Information (STINFO), COMDTINST M5260.6 (series)
(b) Executive Orders (EO): 12356, 12829, 13292/12958
(c) U.S. Code 22 USC Sec. 2751, 2778, 2779, 2780, and 2794
(d) STINFO Markings Process Guide, CGTO PG-85-00-290
(e) National Industrial Security Program Operating Manual, DoD 5220.22M

1. In accordance with reference (a), you are designated as the LC/C4ITSC/Unit (Insert Name) STINFO Manager/Reviewer. Your responsibilities include ensuring that all technical data, technical documents and technical information as defined in references (a) and (e) are marked with the predetermined STINFO Markings prior to distribution beyond the originator of the information.

2. Your designation may not be delegated. The designation of the LC/C4ITSC/Unit (Insert Name) STINFO Manager/Reviewer will be documented within your training file.

3. The LC/C4ITSC/Unit (Insert Name) is committed to maintaining the security of Unclassified Limited-Access STINFO in accordance with references. This is accomplished by the assignment of the STINFO Markings by the originator of the technical information that may include as applicable: a classification marking, Distribution Statement, Export-Control Warning Statement, Destruction Notice and Intellectual Property Notice.

INTENTIONALLY LEFT BLANK

CG/DoD Distribution Statement Levels/Codes					
A	**B**	**C**	**D**	**E**	**F**
					X
				X	
	X				
			X		
	X				
					X
					X
	X				
				X	
				X	
	X				
			X		
		X			
					X
			X		
		X			