

Controlled Unclassified Information Guide

Program: Biological Technologies Office for Guide for Open BAA
Program Security Officer: Jesse Watkins



Version: 1

Mr. Jesse Watkins
BTO Program Security Officer

Dr. Michael Koeris
BTO Office Director

This document is not approved for public release
Local reproduction of this document is authorized only in its entirety.

TABLE OF CONTENTS

(U) FOREWORD	iii
1. (U) PURPOSE	4
2. (U) APPLICABILITY AND SCOPE	4
3. (U) OFFICE OF PRIMARY RESPONSIBILITY (OPR)	4
4. (U) CONTROLLED UNCLASSIFIED INFORMATION (CUI) CHALLENGES.....	4
5. (U) OPERATIONS SECURITY (OPSEC)	5
7. (U) FREEDOM OF INFORMATION ACT (FOIA) EXEMPT INFORMATION.....	6
8. (U) DISCLOSURE of CUI.	7
9. (U) CUI PROTECTION REQUIREMENTS	7
10. (U) NOTIFICATION OF UNAUTHORIZED DISCLOSURE.....	7
11. (U) INFORMATION PROTECTION GUIDANCE CHARTS	7
12. (U) DEFINITIONS.....	9
13. (U) ACRONYMS	9
14. (U) CUI Information Protection Guidance Chart	11

(U) FOREWORD

(U) This guide will contain the baseline instructions of how to mark administrative and financial information within programs, projects, seedlings, studies, SBIRs/STTRs, or other types of work within DARPA BTO covering the range from UNCLASSIFIED through Acknowledged Special Access Programs (SAPs). These instructions will be applicable to the Biological Technologies Office (BTO) to ensure uniformity across BTO security classification guides (SCGs). This plan is based on Department of Defense (DoD) Directives, DARPA Security Guide, and DARPA OPSEC Plan. Any program specific controlled unclassified information (CUI) items or controlled technical information (CTI) will be published in a separate program CUI guide (CUIG).

(U) This guide is not meant to be all-encompassing and does not cover all information that may be protected as CUI. Consult the CUI registry located at <http://www.archives.gov/cui/registry/category-list.html> to verify information not addressed in this guide.

1. (U) PURPOSE

- a. (U) The purpose of this CUIG is to ensure the uniformity in marking and categorization of CUI IAW DoDI 5200.48. Information should be controlled and stored consistent with federal requirements and guidance from the National Institute for Standards and Technology (NIST). Sensitive information does not include information in the public domain.
- b. (U) This guide is not for classified national security information as defined in Executive Order 13526, but identifies specific elements of sensitive information that are unclassified in nature requiring protection. This information is not classified national security information, but it is covered by the legislation at large for the Freedom of Information Act (FOIA) and the exemptions therein.

2. (U) APPLICABILITY AND SCOPE

- a. This guide applies to all BTO Controlled Unclassified Information. This guide should be cited as the basis for identifying, protecting and marking of information and material designated as a type of CUI. As defined at 32 CFR Section 2002.4(h), CUI is information that the government creates or possesses – or that an entity creates or possesses on behalf of the government that law, regulation or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. It is to be used in conjunction with related security classification guides and guidance documents associated with the overall program efforts in compliance with Executive Orders and related DoD guidance. The scope of this guide is based on standardization of BTO CUI markings as planned at the date of this guide, and may expand or change as strategic decisions are made by the BTO Office Director in consultation with the BTO PSO. If a SCG requires stricter protection measures, protect in accordance with stricter guidance.
- b. This guide does not provide guidance on all categories of CUI. There are categories that will differ across programs and will be addressed in detail in the program specific CUIG or SCG, if applicable. Examples of categories not addressed, but not limited to, are Controlled Technical Information and Export Controlled.

3. (U) OFFICE OF PRIMARY RESPONSIBILITY (OPR)

(U) This CUI guide is issued by the DARPA BTO Director. All inquiries concerning content, interpretations, and clarification of this document should be addressed to the BTO PSO at bto_security@darpa.mil.

4. (U) CONTROLLED UNCLASSIFIED INFORMATION (CUI) CHALLENGES

(U) CUI Challenges: Authorized holders of CUI who, in good faith, believe that a designation of information as CUI within this guide is improper or incorrect, or who believe they have received unmarked CUI, should notify the BTO PSO at bto_security@darpa.mil. Until the challenge is resolved, the challenged CUI, including challenges to unmarked CUI, will continue to be

safeguarded and disseminated at the appropriate control level indicated in the markings or presumed category.

5. (U) OPERATIONS SECURITY (OPSEC)

a. (U) OPSEC is a process that identifies and mitigates adversarial risk to our operations by looking at our operations through the eyes of our adversaries. The application of the OPSEC methodology includes identifying critical information, analyzing threats and vulnerabilities, analyzing and assessing adversarial risk, and implementing OPSEC measures that reduce this risk.

b. (U) Collateral and acknowledged SAP SCG categories marked critical information falls under the following index of CUI:

- 1) (U) Organizational Index Grouping: Defense, Export Control, Financial, Intelligence, and Privacy.
- 2) (U) CUI categories: DoD Critical Infrastructure Security Information, General Financial Information, Operational Security, Contract Use.

6. (U) CUI Categories

a. (U) Controlled Technical Information (CTI): Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

b. (U) Defense: DoD Critical Infrastructure Security Information (DCRIT). Information that, if disclosed, would reveal vulnerabilities in the DoD critical infrastructure and, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities, including information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected systems owned or operated on behalf of the DoD, including vulnerability assessments prepared by or on behalf of the DoD, explosives safety information (including storage and handling), and other site- specific information on or relating to installation security.

c. (U) Export Control (EXPT): Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives.

d. (U) Export Controlled Research (EXPTR): Related to the systematic investigation into and study of materials and sources in order to establish facts and reach new conclusions.

e. (U) Financial: General Financial Information (FNC). Related to the duties, transactions, or otherwise falling under the purview of financial institutions or United States Government fiscal functions. Uses may include, but are not limited to, customer information held by a financial institution.

f. (U) General Proprietary Business Information (PROPIN): Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications.

g. (U) Intelligence: Operational Security (OPSEC). This category relates to critical information determined to give evidence of the planning and execution of sensitive (frequently classified) government activities after going through a formal systematic vetting process in accordance with National Security Decision Directive Number 298. This process identifies unclassified information that must be protected. It almost always results from an agency's official OPSEC program, or is otherwise commonly approved for use by the CUI Senior Agency Official.

h. (U) Privacy: Contract Use (CONTRACT). Stipulations for a contractor to meet before material may be used in performance of certain contracts.

i. (U) Privacy: General Privacy (PRVCY). Refers to personal information, or, in some cases, "personally identifiable information," as defined in OMB M-17-12, or "means of identification" as defined in 18 USC 1028.

j. (U) Procurement and Acquisition: Procurement (PROCURE). Material and information relating to, or associated with, the acquisition and procurement of goods and services, including but not limited to, cost or pricing data, contract information, indirect costs and direct labor rates.

k. (U) Procurement and Acquisition: Small Business and Technology (SBIZ). Relating to certain "Small Business Innovation Research Program" and "Small Business Technology Transfer Program" information in a government database, as referenced in 15 USC 638(k)(2).

l. (U) Procurement and Acquisition: Source Selection (SSEL): Any information that is prepared for use by an agency for the purpose of evaluating a bid or proposal to enter into an agency procurement contract, if that information has not been previously made available to the public or disclosed publicly.

7. (U) FREEDOM OF INFORMATION ACT (FOIA) EXEMPT INFORMATION

(U) The Freedom of Information Act (FOIA), 5 U.S.C. § 552, is a federal law that defines agency records subject to public disclosure, outlines mandatory disclosure procedures, and defines nine exemptions that prohibit certain types of information from being released to the public. In addition to the FOIA, the Code of Federal Regulations (October 2016), 45 CFR § 5.31 specifies the type of information that falls under each of the nine exemptions that preclude release of information to the public under the FOIA. In accordance with 5 U.S.C. § 552(a)(8), DARPA will withhold records or information exempt from disclosure under the FOIA whenever disclosure would harm an interest protected by a FOIA exemption or disclosure is prohibited by law.

8. (U) DISCLOSURE of CUI.

a. (U) Public Disclosure. DoD information requested by the media or members of the public or proposed for release to the public by DoD civilians or military personnel or their contractors will be processed in accordance with DARPA Instruction 65 and DoD Instructions 5230.09, 5230.29; Volume 3 of DoD Manual 5200.01; and DoD Manual 5400.07, as applicable. Proposed public disclosures of unclassified information shall be submitted using the public release form located at <https://www.darpa.mil/work-with-us/contract-management/public-release>.

b. (U) Freedom of Information Act (FOIA) Requests. All personnel with knowledge of this Project must coordinate through the DARPA, BTO ADPM prior to providing a response to requests for information under the provisions of the FOIA.

c. (U) Proprietary Information (PROPIN). Additional safeguards may become necessary if a contract requires the transfer of PROPIN. The holder of the information must clearly identify any and all PROPIN prior to its disclosure and release, the release will be coordinated with the PROPIN owner.

d. (U) Foreign Disclosure. Disclosure of DARPA CUI to foreign nationals will be coordinated with the PSO, International Security, and International Cooperation. Disclosure approval must be granted by the Director, SID, who is the Foreign Disclosure Officer for DARPA.

9. (U) CUI PROTECTION REQUIREMENTS

a. (U) CUI (e.g., confidential business information, PII, etc.) regardless of media or format, will be protected from disclosure to unauthorized persons or groups, by properly storing in locked offices, cabinets, and drawers in accordance with DoDI 5200.48.

b. (U) CUI may only be processed on DIB systems that are compliant with DFARS 252.204-7012 requirements as detailed in NIST 800-171.

10. (U) NOTIFICATION OF UNAUTHORIZED DISCLOSURE

a. (U) Personnel must immediately report all unauthorized disclosures or suspected and known security incidents, privacy breaches, and suspicious activities involving CUI to the BTO PSO jesse.watkins@darpa.mil.

b. (U) Data breaches of DIB networks and systems involving CUI material must be reported IAW DFARS 252.204-7012 requirements. In addition, all breaches must be reported to the DARPA Project contracting officer and program security officer (PSO) upon discovery.

11. (U) INFORMATION PROTECTION GUIDANCE CHARTS

a. These charts (see Table 1 below) are provided to assist in identifying what types of information within BTO CUIGs, collateral and acknowledged SAP SCGs that are at a minimum

protected as CUI, provide guidance on the relevant markings for this information to control dissemination, and provide guidance on when these dissemination controls no longer apply.

b. (U) This chart is not all-encompassing and does not cover all information that may be protected as CUI. Consult the CUI registry located at <http://www.archives.gov/cui/registry/category-list.html> to verify information not addressed below. If at any time there are questions regarding which category of information something falls under, or what dissemination controls apply, individuals should request guidance from their program PSR or the BTO PSO.

c. (U) The items in the table below are items BTO has identified at a minimum to be CUI. Combined with additional information some may be classified at a higher level. Please work with your PSR and PSO to ensure information is protected at the proper level.

12. (U) DEFINITIONS

- a. (U) Budget Identifier – unclassified name assigned by the Tech Office ADPM for DARPA SAPs. This name has no relation to the program technical details. Budget Identifiers (BIDs) are not OSD SAPCO or Joint Chiefs of Staff assigned nicknames.
- b. (U) Controlled Technical Information – technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
- c. (U) Controlled Unclassified Information – is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.
- d. (U) Limited Dissemination Control – is any CUI Executive Agent (EA)-approved control that agencies may use to limit or specify CUI dissemination.
- e. (U) Performer Issued Name – program name assigned by a performer used to identify a SAP for internal use among that performer.
- f. (U) Pre-Decisional Budget – program budgets and pending budget requests to an agency that are not approved or have not been formally submitted and approved.
- g. (U) Program Identifier – SAPCO assigned number used to identify SAPs; used in portion marking SAP documents.
- h. (U) Proprietary Information – information (whether now existing or hereafter created or acquired) developed, created, or discovered by the Company, or which became known by, or was conveyed to the Company, which has commercial value in the Company's business.
- i. (U) Special Access Program – a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

13. (U) ACRONYMS

- a. (U) ADPM Assistant Director, Program Management
- b. (U) BID Budget Identifier
- c. (U) BTO Biological Technologies Office
- d. (U) CFR Code of Federal Regulations
- e. (U) CTI Controlled Technical Information
- f. (U) CUI Controlled Unclassified Information
- g. (U) CUIG Controlled Unclassified Information Guide
- h. (U) DARPA Defense Advanced Research Projects Agency

i.	(U)	DFARS	Defense Federal Acquisition Regulation Supplement
j.	(U)	DIB	Defense Industrial Base
k.	(U)	DoD	Department of Defense
l.	(U)	DoDI	Department of Defense Instruction
m.	(U)	DoDM	Department of Defense Manual
n.	(U)	FOIA	Freedom of Information Act
o.	(U)	IAW	in accordance with
p.	(U)	LDC	Limited Dissemination Control
q.	(U)	NIST	National Institute of Standards and Technology
r.	(U)	OMB	Office of Management and Budget
s.	(U)	OPSEC	Operational Security
t.	(U)	PI	Proprietary Information
u.	(U)	PID	Program Identifier
v.	(U)	PSO	Program Security Officer
w.	(U)	PSR	Program Security Representative
x.	(U)	RFI	Request for Information
y.	(U)	SAP	Special Access Program
z.	(U)	SAPF	Special Access Program Facility
aa.	(U)	SAPCO	Special Access Program Central Office
bb.	(U)	SBIR	Small Business Innovation Research
cc.	(U)	SBTT	Small Business Technology Transfer
dd.	(U)	SCG	Security Classification Guide
ee.	(U)	SID	Security and Intelligence Directorate (DARPA)
ff.	(U)	USC	United States Code

14. (U) CUI Information Protection Guidance Chart

Table is: UNCLASSIFIED

Element of Information	Index	Category	Reason	LDC or Distribution Statement	Remarks
Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.	Defense	Controlled Technical Information (CTI)	48 CFR 252.204-7012	DISTRO B-F, IAW DoDI 5230.24	FOIA Exemption 3 may be applicable. ITAR and EAR
Systematic investigation into and study of materials and sources in order to establish facts and reach new conclusions. * Does not apply to 6.1 Fundamental Research, unless otherwise agreed upon between DARPA and the performer.	Export Controlled Research	Export Controlled Research (EXPTR)	15 CFR 734.8(b)	DISTRO B-F IAW DoDI 5230.24	For 6.2 Applied Research; control as EXPTR pending prepublication review and approval for public release.
Information or data defined within the Commerce Control List (CCL), United States Munitions List (USML), or applied license applications to control export.	Export Control	Export Controlled	"50 USC 4614(c); 13 USC 301(g); 42 USC 2156; 42 USC 2168(a); 22 CFR 124.9(a)(5); 50 USC 4605(l)(5); 10 USC 130(a); 32 CFR 250.4(a)	DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government Agencies and their contractors, Export Controlled, (Date). Other requests shall be referred to	FOIA Exemption 3 may be applicable. ITAR and EAR All material with export controls will also post the following notice: ("WARNING - This document

			// 42 USC 2077(a); 15 CFR 718.3; 22 CFR 126.10(b); 15 CFR 748.1(c); 15 CFR	DARPA, Biological Technologies Office.	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 Control Reform Act of 2018 (Title 50, U.S.C., Chapter 58, Sec. 4801-4852). Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.")
Non-public data controlled by the business or individual as proprietary	Proprietary Business Information	General Proprietary Business Information (PROPIN)	18 USC 1905 29 USC 664	Federal Employees and Contractors Only (FEDCON)	FOIA Exemption
Personal Identifiable Information (PII)	Privacy	PRVCY	Privacy Act of 1974	FEDCON	FOIA Exemption 6 may be applicable.
Personal Health Information (PHI)	Privacy	HLTH	Privacy Act of 1974	FEDCON	FOIA Exemption 6 may be applicable.

Table is: UNCLASSIFIED