Controlled Unclassified Information Guide

Program: Faithful Integrated Reverse-engineering and Exploitation (FIRE)
Program Manager: Lok K. Yan
Program Security Officer: James Persons

Date: February 24, 2023
Version: 1.0

YAN.LOK.K.1268145954 Digitally signed by YAN.LOK.K.1268145954 Date: 2023.02.24 13:49:22 -05'00'

Lok K. Yan, Ph. D.
Program Manager

PERSONS.JAMES.KENNETH.1214880993 Digitally signed by PERSONS.JAMES.KENNETH.1214880993 Date: 2023.02.24 13:22:41 -05'00'

Mr. James K. Persons
Program Security Officer

PREDECISIONAL

FOREWORD

GENERAL

FOREWORD

1. DESCRIPTION

The objective of the FIRE program is to develop tools to find, exploit, and patch vulnerabilities in medium-complexity cyber-physical systems within a month from when an analysis team receives the physical system. FIRE is primarily interested in vulnerabilities that arise from the composition of hardware, software and physical sub-systems where each component may not be vulnerable in-and-of itself; vulnerabilities in individual sub-systems (e.g., software only) are of secondary interest.

a. Definition for defining CUI Table:

1.) Non-Commercial systems are considered systems used by the government that can be in the form of components integrated into a device, a system used by the government, government furnished equipment, or government furnished software.

2.) Preparation is defined as time needed to identify components, their inter-dependencies, sensor placements and configurations.

2. AUTHORITY

CUI elements referenced in this guide are under the authority of DoDI 5200.48, “Controlled Unclassified Information,” March 6, 2020.

3. DISTRIBUTION

Distribution unlimited, approved for public release.

GENERAL

1. PURPOSE

   a. The purpose of this controlled unclassified information (CUI) guide is to ensure the protection of information IAW DoDI 5200.48. This 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. 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 but still require 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, Patents filled under 35 U.S.C. 111(a), Export controlled International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR), Proprietary Manufacturer, and General Proprietary Business Information.

2. APPLICABILITY AND SCOPE

This guide applies to all DARPA personnel, support contractors, mission partners, and industrial performers who develop material in response and support to FIRE. This guide should be cited as the basis for identifying, protecting, and marking of information and material designated as a type of Controlled Unclassified Information (CUI) associated with FIRE. 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 effort of FIRE, in compliance with Executive Orders and related DoD guidance. The scope of this guide is based on MTO solicitations or requests as planned at the date of this guide, and may expand or change as strategic decisions are made over the course of FIRE.

3. OFFICE OF PRIMARY RESPONSIBILITY (OPR)

This CUI guide is issued by DARPA. All inquiries concerning content, interpretations, and clarification of this document should be addressed to DARPA at MTOSecurity@darpa.mil.

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

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 DARPA at MTOSecurity@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. OPERATIONS SECURITY (OPSEC)

a. 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. FIRE critical information falls under general use the following index of CUI:

    1) Defense

    2) Critical Infrastructure

    3) Proprietary Business Information

6. CUI Categories

a. Defense: Controlled Technical Information (CTI). This category relates to technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet that criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents.

b. Critical Infrastructure: Information Systems Vulnerability Information. This category relates to information that if not protected, could result in adverse effects to information systems. Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

c. Proprietary Business Information: 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.

7. EXPORT CONTROL RESTRICTED INFORMATION

FIRE should not contain export control restricted information which includes research information pertaining to Export Administration Regulations. If export control information is identified by performer, the performer will notify the DARPA Project contracting officer and MTO program security officer (PSO) upon discovery at MTOSecurity@darpa.mil.

8. FREEDOM OF INFORMATION ACT (FOIA) EXEMPT INFORMATION

a. 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. The most relevant exemptions for FIRE are listed below; however other exemptions could apply:

    1) Exemption 3 – Protects information exempted from release by statute.

    2) Exemption 4: Trade secrets or commercial or financial information that is confidential or privileged.

9. DISCLOSURE of CUI.

a. Public Disclosure. Information from this CUI guide does not allow automatic public release of this information. 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. Freedom of Information Act (FOIA) Requests. All personnel with knowledge of this Project must coordinate with the DARPA PSO prior to providing a response to requests for information under the provisions of the FOIA.

c. Proprietary Information. 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. Release will be coordinated with the PROPIN owner.

d. 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.

10. CUI PROTECTION REQUIREMENTS

a. FIRE CUI (e.g., General Proprietary Business Information and Export Controlled), 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. CUI may only be processed on DIB systems that are compliant with DFARS 252.204-7012 requirements, as detailed in NIST 800-171.

11. NOTIFICATION OF UNAUTHORIZED DISCLOSURE

a. Personnel must immediately report all unauthorized disclosures or suspected and known security incidents, privacy breaches, and suspicious activities involving CUI to the FIRE security team at MTOSecurity@darpa.mil.

b. Data breaches of DIB networks and systems involving FIRE 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 MTO program security officer (PSO) upon discovery at MTOSecurity@darpa.mil.

EXAMPLE DISTRIBUTION BLOCK

Controlled by: DARPA
Controlled by: MTO
CUI Category: Information Systems Vulnerability Information
Distribution/Dissemination Control: FEDCON
POC: [last person to edit items name and phone or email address]

12. INFORMATION PROTECTION GUIDANCE CHARTS

These charts are provided to assist in identifying what types of information associated with the MTO solicitation or request effort may be sensitive, provide guidance on the relevant markings for this information to control dissemination, and provide guidance on when these dissemination controls no longer apply. 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 DARPA at MTOSecurity@darpa.mil.

The distribution statements below do not supersede existing statements and limitations if they already exist.

Element of Information	**Index**	**Category**	**Reason**	**LDC or Distribution Statement**	**Remarks**
Information or data on confirmed vulnerabilities, exploits, and its patches in information systems	Critical Infrastructure	Information Systems Vulnerability Information	44 USC 3554 (OMB M-17-05 implementing guidance); 44 USC 3555(f)	Federal Employees and Contractors Only (FEDCON) DISTRIBUTION STATEMENT D: Distribution authorized to Department of Defense and U.S. DoD contractors only [category] [date of determination]. Other requests for this document must be referred to [controlling DoD office]	FOIA Exemption 3 may be applicable Information or data on DARPA provided systems is UNCLASSIFIED Commercial information systems will use FEDCON LDC. CUI Designation block found above. Commercial components known to be integrated in DoD components will use DISTRIBUTION STATEMENT D.

Information or data regarding hardware that does not expose a vulnerability or exploit is considered UNCLASSIFIED, unless that hardware is non-commercial	Defense	Controlled Technical Information	48 CFR 252.204-7012; Title 10, § 130; 31 CFR 800.209; Parts 22 CFR 120-130; 15 CFR 730-774; 22 USC 2778 (AECA); Export Control Reform Act of 2019 (FY 2019 NDAA, Subitle B - Sections 1741-1781/PL 115-232);10 USC 130(a) (DoD authority to withhold export controlled space/mil info); 32 CFR 250 // DoDD 5000.01; DoDD5000.02; DoDI 5200.39; DoD Directive 5230.25; DoDI 3200.12	DISTRIBUTION STATEMENT D. Distribution authorized to Department of Defense and U.S. DoD contractors only [category] [date of determination]. Other requests for this document must be referred to [controlling DoD office]	FOIA Exemption 3 may be applicable
Information or data regarding software that does not expose a vulnerability or exploit is considered UNCLASSIFIED, unless that software is non-commercial	Defense	Controlled Technical Information	48 CFR 252.204-7012; Title 10, § 130; 31 CFR 800.209; Parts 22 CFR 120-130; 15 CFR 730-774; 22 USC 2778 (AECA); Export Control Reform Act of 2019 (FY 2019 NDAA, Subitle B - Sections 1741-1781/PL 115-232);10 USC 130(a) (DoD authority to withhold export controlled space/mil info); 32 CFR 250 // DoDD 5000.01; DoDD5000.02; DoDI 5200.39; DoD Directive 5230.25; DoDI 3200.12	DISTRIBUTION STATEMENT D. Distribution authorized to Department of Defense and U.S. DoD contractors only [category] [date of determination]. Other requests for this document must be referred to [controlling DoD office]	FOIA Exemption 3 may be applicable
Modeling tools are UNCLASSIFIED	N/A	N/A	N/A	N/A	N/A

Modeling of systems is UNCLASSIFIED provided data is not used to confirm a vulnerability, exploit, or patch	Critical Infrastructure	Information Systems Vulnerability Information	44 USC 3554 (OMB M-17-05 implementing guidance); 44 USC 3555(f)	Federal Employees and Contractors Only (FEDCON) DISTRIBUTION STATEMENT D: Distribution authorized to Department of Defense and U.S. DoD contractors only [category] [date of determination]. Other requests for this document must be referred to [controlling DoD office]	FOIA Exemption 3 may be applicable Information or data on DARPA provided systems is UNCLASSIFIED Commercial information systems will use FEDCON LDC. CUI Designation block found below. Commercial components known to be integrated in DoD components will use DISTRIBUTION STATEMENT D.
Simulation tools are UNCLASSIFIED	N/A	N/A	N/A	N/A	N/A
Simulation of systems is UNCLASSIFIED provided data is not used to confirm a vulnerability, exploit, or patch	Critical Infrastructure	Information Systems Vulnerability Information	44 USC 3554 (OMB M-17-05 implementing guidance); 44 USC 3555(f)	Federal Employees and Contractors Only (FEDCON) DISTRIBUTION STATEMENT D: Distribution authorized to Department of Defense and U.S. DoD contractors only	FOIA Exemption 3 may be applicable Information or data on DARPA provided systems is UNCLASSIFIED Commercial information systems will use FEDCON

				[category] [date of determination]. Other requests for this document must be referred to [controlling DoD office]	LDC. CUI Designation block found below. Commercial components known to be integrated in DoD components will use DISTRIBUTION STATEMENT D.
Preparation tools are UNCLASSIFIED	N/A	N/A	N/A	N/A	N/A
Preparing systems for vulnerability analysis is UNCLASSIFIED provided those systems are non-commercial	N/A	N/A	N/A	N/A	Non-commercial systems may require CUI controls in accordance with (IAW) this CUI guide
Engineering Support provided for commercial, non-government systems is UNCLASSIFIED	N/A	N/A	N/A	N/A	Non-commercial systems may require CUI controls in accordance with (IAW) this CUI guide
Non-public data controlled by the a 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 4 may be applicable.