Controlled Unclassified Information Guide

Decentralized Artificial Intelligence via Controlled Emergence (DICE)
Program Manager: Dr. Susmit Jha
Program Security Officer: Justin Kokernak

Date: April 2026
Version: 1

JHA.SUSMIT.KUMAR.1616933350 Digitally signed by JHA.SUSMIT.KUMAR.1616933350 Date: 2026.04.13 11:49:43 -04'00'

Dr. Susmit Jha
I2O Program Manager

KOKERNAK.JUSTIN.PAUL.1288186037 Digitally signed by KOKERNAK.JUSTIN.PAUL.1288186037 Date: 2026.04.15 10:52:24 -04'00'

Justin Kokernak
I2O Program Security Officer

FOREWORD

GENERAL

FOREWORD

1. DESCRIPTION

Decentralized Artificial Intelligence via Controlled Emergence (DICE) will develop theory and algorithms for decentralized self-organization to enable a scalable, adaptive and resilient multi-agent AI collective of heterogeneous AI agents that can autonomously execute sustained long-time horizon multi-step missions in contested environments.

2. AUTHORITY

CUI elements referenced in this guide are under the authority of Executive Order 13556, Controlled Unclassified Information, November 4, 2010 (as amended) and in accordance with DoDI 5200.48, “Controlled Unclassified Information,” March 6, 2020.

3. DISTRIBUTION:

Distribution Statement A: Approved for public release, distribution unlimited.

GENERAL

1. PURPOSE

a. The purpose of this CUI guide is to ensure the protection of Decentralized Intelligence via Controlled Emergence (DICE) information IAW DoDI 5200.48. DICE information must be controlled and stored consistent with DFARS 252.204-7012 requirements as detailed in National Institute for Standards and Technology (NIST) 800-171.

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 but require additional protections.

2. APPLICABILITY AND SCOPE

This guide applies to information, material and processes generated by DICE. This guide is the basis for identifying, protecting and marking information and material designated as a type of controlled unclassified information (CUI) associated with DICE. This guide is used in conjunction with related guidance (security classification guides, DoW Policy, etc.) associated with the overall effort of DICE. The scope of this guide is based on DICE as planned at the date of this guide and may change over the course of DICE.

3. OFFICE OF PRIMARY RESPONSIBILITY (OPR)

The Office of Primary Responsibility is the Information Innovation Office at I2OSecurity@darpa.mil.

4. CONTROLLED UNCLASSIFIED INFORMATION (CUI) CHALLENGES

CUI Challenges are directed to the OPR. Information is protected in accordance with this guide until the challenge is resolved.

5. CUI CATEGORIES. The following CUI Categories are used to protect DICE:

a. Intelligence: Operational Security (OPSEC). 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 Presidential Memorandum 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.

b. Defense: Controlled Technical Information (CTI). Controlled Technical Information means 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 is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24,

"Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

6. EXPORT CONTROL RESTRICTED INFORMATION

Each performer is responsible for assessing their technology and ensuring compliance with all export control laws and regulations. This CUI guide does not relieve any program participant from export control requirements.

7. DISCLOSURE of CUI

a. Public Disclosure. Public Disclosure of any DICE information must follow the DISTAR process. Please contact the DICE OPR and Public_Release_Center@darpa.mil for additional guidance.

b. Freedom of Information Act (FOIA) Requests. All FOIA requests are directed to the DARPA FOIA Office.

c. Foreign Disclosure. CUI controlled by DARPA may be shared with foreign nationals if access to such information would accomplish a lawful government purpose and would not be detrimental to national security.

8. CUI PROTECTION REQUIREMENTS

DICE CUI must be stored in accordance with DODI 5200.48. Processing of CUI is only authorized on systems compliant with DFARS 252.204-7012 as detailed in NIST 800-171.

9. UNAUTHORIZED DISCLOSURE

a. Personnel must immediately report all unauthorized disclosures or suspected and known security incidents, and suspicious activities involving CUI to the DICE PSO and PSR at I2OSecurity@darpa.mil.

b. Data breaches of Defense Industrial Base (DIB) networks and systems involving DICE 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.

10. INFORMATION PROTECTION GUIDANCE CHARTS

These charts are provided to assist in identifying what types of information associated with the DICE 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 the DICE PSR at I2OSecurity@darpa.mil.

Element of Information	**Index**	**Category**	**Reason**	**LDC or Distribution Statement**	**Remarks**
All documentation, system outputs, test results and work products related to the application of any program-developed algorithm, technique, or capability for a DoW relevant platform or dataset.	Defense	CTI	DFARS 252.204.7012 DoDI 5230.24	DISTRO C	
Performance metrics and evaluation data for AI-related software integrated into, trained on or tested on any DoW system or mission.	Defense	CTI	DFARS 252.204.7012 DoDI 5230.24	DISTRO C	
Individual AI models or multi-agent AI model collectives trained or fine-tuned on data sets derived from DoW sources.	Defense	CTI	DFARS 252.204.7012 DoDI 5230.24	DISTRO C	
Data sets derived from DoW sources.	Defense	CTI	DFARS 252.204.7012 DoDI 5230.24	DISTRO C	

Algorithms required for AI to conduct formal reasoning and make inferences and predictions that contain logic specific to DoW systems or applications.	Defense	CTI	DFARS 252.204.7012 DoDI 5230.24	DISTRO C	
Simulation environments for military training, military scenarios or simulating any defense articles.	Defense	CTI EXPT	USML Category IX: Military Training Equipment and Training	DISTRO C	
Model weights of any closed-weight AI model (i.e., not published) that has been trained on more than 10^{26} computational operations.	Defense	CTI EXPT	CCL: ECCN 4E091	DISTRO C	
Identification of specific DoW systems or applications that DICE technology will be deployed in.	Intelligence	OPSEC	NSDD 298	FEDCON	