Controlled Unclassified Information Guide

Program: Resilient Anonymous Communication for Everyone (RACE)

Program Manager: Dr. Joshua Baron

Program Security Officer: Denice Holden

Date: June 6, 2018

Version: 1.0

1 Background

The Resilient Anonymous Communication for Everyone (RACE) program will research technologies for a distributed messaging system that a) can exist completely within a given network, b) provides confidentiality, integrity, and availability of messaging, and c) preserves privacy to any participant in the system. Compromised system data and associated networked communications should not be helpful to compromise any additional parts of the system. RACE advances will be based on rigorous security arguments, such as those found in the academic cryptography community or statistical arguments based on realistic simulations. RACE will create advances in communication protocol encapsulation methods as well as efficient, oblivious, distributed system tasking, possibly via secure multiparty computation, to build a system that cannot be compromised even with limited participant compromises and large-scale, real-time deep packet inspection.

2 Purpose

This guide identifies those aspects of the program that performers must handle as Controlled Technical Information (CTI). Questions concerning the content and interpretation of this guide and/or recommendations for changes due to current conditions, progress made in program research, scientific technological developments, advances in state of the art, or other factors should be directed to the DARPA Program Manager. All users of this guide are encouraged to assist in improving its currency and adequacy. No changes are approved until DARPA issues an official modification and updates this guide.

3 Definition of Controlled Technical Information for the Program

DoD considers “technical information” to be 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 code. Note that such technical information may or may not be controlled (i.e., CTI), depending on whether it has military or space application.

Controlled Technical Information (CTI) is defined as technical information with military or space application that is subject to controls on its access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. CTI is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements on Technical Documents." The term CTI does not apply to information that is lawfully publicly available without restrictions.

For the RACE Program, DARPA considers that all documentation, system outputs, test results, and work products solely related to the application of any program-developed algorithm, technique, or capability to a specific military system to be at least CTI. Such detailed technical information could reveal sensitive or even classified capabilities and/or vulnerabilities of that military system. As an example, an Android application developed solely for use by US military forces would be CTI. However, an application developed for commercial use would not be CTI.

The application programming interfaces (APIs) user interfaces, and assembled systems will constitute CTI if the APIs user interfaces, or assembled systems directly incorporate material from CUI or CTI sources. The evaluation planning, performance results, and user observation or testing results based on CUI transition partner data will also constitute CUI. The datasets and other materials prepared for RACE will constitute CTI if they directly incorporate material from CUI or CTI sources. In addition, datasets or other information received from transition partners will constitute CTI if the originator of the dataset or the RACE PM designates it as such.

4 Safeguarding CTI

The Contractor shall protect CTI in accordance with DFARS 252.204-7012. Contractor information systems shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations". DARPA can provide general guidance on how to implement 800-171 controls.

5 Aspects of the Program that Will Not Involve CTI

5.1 Program Management

- Information and materials related to program schedules, meeting plans, programmatic goals and intentions, research directions, strategic challenges and gaps, instructions, status updates, and other such program management information and materials, whether created by DARPA or performers, will not constitute CTI unless they include material deemed to be CUI as noted in Section 3 of this guide.
- Non-CTI RACE management information and material may be shared with any program participant, U.S. government representative, or other authorized individual or group by any means of communication, including in-person discussion, telephone communication, electronic message, electronic or hardcopy document, or electronic sharing medium.

5.2 Interaction and Collaboration

- Frequent and extensive interaction and collaboration among performers is a crucial program activity. Information and materials related to RACE research, development, software and system details, data preparation, algorithm performance, strategic objectives, and other such RACE technical information and materials, whether created by DARPA or performers, will not constitute CTI unless they include material deemed to be CUI as noted in Section 3 of this guide.
- Non-CTI RACE interaction and collaboration information and material may be shared with any program participant, U.S. government representative, or other authorized individual or group by any means of communication, including in-person discussion, telephone communication, electronic message, electronic or hardcopy document, or electronic sharing medium. When at all possible, encryption of data at rest and in motion is highly encouraged.

5.3 Evaluation and Assessment

- Information and materials related to RACE evaluation or assessment planning, execution, or results, whether created by DARPA or performers, will not constitute CTI unless they include material deemed to be CUI as noted in Section 3 of this guide.
- Non-CTI RACE evaluation and assessment information and material may be shared with any program participant, U.S. government representative, or other authorized individual or group by any means of communication, including in-person discussion, telephone communication, electronic message, electronic or hardcopy document, or electronic sharing medium. When at all possible, encryption of data at rest and in motion is highly encouraged.

DARPA considers that all documentation, system outputs, test results, and work products that are not solely related to the application of any program-developed algorithm, technique, or capability to a specific military system are not CTI.

By Technical Area, the following work products are not CTI, either individually or in combination with other non-CTI RACE-developed technologies, provided they are not solely intended to be used on a specific military system:

5.4 TA1: Cryptography

- Techniques, documentation (to include security proofs), protocols, and software to perform secure multiparty computation, including underlying primitives (e.g., secret sharing, homomorphic encryption, etc.)
- Any further cryptographic functionalities to enabled RACE capabilities, to enable cryptographic key exchange

5.5 TA2: Communication Obfuscation

- Techniques, documentation (to include security proofs), protocols, and software to encapsulate or otherwise obfuscate communication within targeted communications channels
- Data obtained by TA2 performers regarding communications channels within which to obfuscate communications, unless identified as CTI by the source of that data

5.6 TA3: System

- Techniques, documentation, protocols, and software that implements the integrated RACE system, to include mobile applications for client communication, applications to execute the distributed means of passing messages between clients
- Techniques for networking to enable the distributed RACE system
- Means of client and/or server application distribution (see also section 5.4)

5.7 TA3.1: Resilient Application Distribution

- Techniques, documentation (to include security proofs), protocols, and software to perform application sharding and reconstruction, including underlying primitives (e.g., secret sharing, application decombination and recombination, etc.)