Controlled Unclassified Information Guide

Program: Computers and Humans Exploring Software Security (CHESS)

Program Manager: Mr. Dustin Fraze

Program Security Officer: Ms. Denice Holden

Date: March 29, 2018

Version: 1.0

1 Background

The CHESS program will develop computer/human systems to rapidly discover all classes of vulnerability in complex software. These novel approaches for the rapid detection of vulnerabilities will focus on identification of system information gaps that require human assistance, generation of representations of these gaps appropriate for human collaborators, capture and integration of human insights into the analysis process, and the synthesis of software patches based on this collaborative analysis. The program will take an experimental approach to verify the effectiveness of such collaborative systems, and to measure their success rate discovering software vulnerabilities in realistic software without affecting production software or deployed systems.

2 Purpose

This guide identifies those aspects of the program that performers must handle as Controlled Technical Information (CTI). In addition, each performer must determine and assert the export controls (either Export Administration Regulations or International Traffic in Arms Regulations) relevant to their project, and communicate that assertion to their contracting agent and the DARPA Program Manager.

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 clauses 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013) and 252.227-7014 “Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation” (48 CFR 252.227-7014). 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 CHESS Program, DARPA considers that all documentation, system outputs, test results, and work products related to the application of any program-developed algorithm, technique, or capability to a militarily relevant platform to be at least CTI. Such detailed technical information could reveal sensitive or even classified capabilities and/or vulnerabilities of that military platform. Additionally, all documentation, system outputs, test results, and work products that identify vulnerabilities in Commercial off the Shelf (COTS), Government off the Shelf (GOTS), or Free and Open Source Software (FOSS) are considered CTI.

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.

As part of their efforts on this program, TA5 performers may apply TA1 and TA2-developed capabilities to one or more militarily relevant platforms, and therefore must be able to meet all CTI safeguarding requirements. TA5 performers shall therefore deliver to DARPA a detailed plan for providing feedback to other performers regarding the performance of their systems without divulging any CTI or classified information. This plan must describe procedures for abstracting system failures and constructing test cases that replicate these failures without recourse to data or information specific to the military platform under test. TA5 performers must submit this plan to DARPA no less than 90 days prior to demonstrations that involve a militarily relevant platform, to allow sufficient time for discussion with the Government team and the completion of any necessary revisions. CTI Information must be handled IAW DoDM 5200.01, Volume 4 – CUI.

5 Aspects of the Program that Will Not Generate CTI

DARPA considers that the algorithms developed on this program will constitute advances to the state of the art and are not CTI when realized in source code or executable formats, or when documented in written reports. The outputs and work products resulting from application of algorithms to non-militarily relevant target platforms are only considered CTI if they identify vulnerabilities in COTS, GOTS, or FOSS software.

In this context, the term *algorithm* is defined as the representation of a sequence of abstract logical and/or mathematical operations performed on data. Any algorithm that must be trained on or configured with respect to particular sets of data to achieve its intended functionality is not CTI in its pre-trained form, but instances of that algorithm that have been trained on or configured by CTI data must be treated as CTI. For example, the algorithms required to train and run a neural network are not considered CTI, but the resulting neural network would be CTI if it were trained on a CTI dataset. Similarly, software for aerodynamic design are generally commercial tools, but a specific design made using the software could be CTI.

The TA3 and TA5 performers will coordinate with the DARPA Program Manager to make available to all other performers unclassified challenge sets and an evaluation environment that is not militarily relevant, to facilitate technology development.

By Technical Area, the following work products are not CTI:

5.1 TA1: Human Collaboration

- Algorithms or data on human behavior analysis related to the reverse engineering or vulnerability discovery processes
- Algorithms to automatically convert program analysis information gaps in into representations for human analysis
- Algorithms to process human feedback into formats for automated program analysis
- Any trained/learned elements of any of the above algorithms and/or data models unless the training is conducted solely with data that includes CUI or can be reasonably attributed to CUI
- Algorithms, scripts, regression unit tests, and documentation that make no reference to systems other than unclassified non-militarily relevant target platforms

5.2 TA2: Vulnerability Discovery

- Algorithms for vulnerability analysis of source code or intermediate build artifacts, including the compiled, stripped binary
- Algorithms for the generation and verification of source code and binary patches
- Synthetic vulnerabilities found in challenge sets
- Any trained/learned elements of any of the above algorithms unless the training is conducted solely with data that includes CUI or can be reasonably attributed to CUI
- Algorithms, scripts, regression unit tests, and documentation that make no reference to systems other than unclassified non-militarily relevant target platforms

5.3 TA3: Voice of the Offense

- Algorithms for generating or inserting synthetic software vulnerabilities into source code or binaries
- Algorithms for synthesizing compound software vulnerabilities with source code or binaries
- Synthetic vulnerabilities found in challenge sets
- Algorithms, scripts, regression unit tests, and documentation that make no reference to systems other than unclassified non-militarily relevant target platforms

5.4 TA4: Control Team

- Synthetic vulnerabilities found in challenge sets
- Algorithms, scripts, regression unit tests, and documentation that make no reference to systems other than unclassified non-militarily relevant target platforms

5.5 TA5: Integration, Test and Evaluation

- Test plans for unclassified non-militarily relevant target platforms
- Evaluation metrics for TA1 and TA2 specific to the unclassified non-militarily relevant target platforms
- Component and system tests for the CHESS integration framework
- Component and system tests for the CHESS testbed environment
- Evaluation approaches for maximizing test coverage of unclassified, non-militarily relevant target platforms
- Algorithms, scripts, regression unit tests, and documentation that make no reference to systems other than unclassified non-militarily relevant target platforms