Controlled Unclassified Information Guide

Program: Configuration Security (ConSec)

Program Manager: Mr. Jacob Torrey

Program Security Officer: Mr. Gregory Woosley

Date: December 4, 2017

Version: 1.0

1 Background

The ConSec program seeks to develop a system to automatically generate, deploy, and enforce configurations of components and subsystems for use in military platforms. By viewing individual component configurations as elements of the overall composed system's behavior and security, more secure system configurations can be developed and deployed to improve security without requiring large hardware changes.

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 to 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 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 include information that is lawfully publicly available without restrictions.

For the ConSec 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 minimum CTI. Such detailed technical information could reveal sensitive or even classified capabilities and/or vulnerabilities of that military platform.

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 guidance on how to implement 800-171 controls.

As part of their efforts on this program, TA1 performers will apply TA2-developed capabilities to one or more militarily relevant platforms, and therefore must be able to meet all CTI safeguarding requirements. TA1 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. TA1 performers must submit this plan to DARPA no less than 90 days prior to commencing work on a militarily relevant platform, to allow sufficient time for discussion with the Government team and the completion of any necessary revisions.

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 not considered CTI. 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.

TA1 performers will coordinate with the DARPA Program Manager to make available to all other performers unclassified target platforms that are not militarily relevant, to facilitate technology development. Specifically by Technical Area, the following work products are not CTI:

5.1 TA1 Understand Composed System

- Operational context-driven system models for target platforms that are not militarily relevant
- Algorithms to automatically generate configuration-aware functional specifications
- Algorithms for converting operational context into domain-specific languages
- Algorithms for analysis of binary and/or source code of components
- Algorithms, scripts, regression unit tests, and documentation that makes no reference to systems other than unclassified non-militarily relevant target platforms

5.2 TA2 Generate Secure Configuration

- Models, simulators and/or distributable prototypes and related APIs developed under the program and specific to unclassified non-militarily relevant target platforms
- Algorithms for generation of mission-optimized configurations
- Simulation algorithms for exploring target platforms to elicit anticipated behaviors
- Algorithms and/or techniques for generation of assurance cases in support of authority-to-operate approval
- Algorithms for context-sensitive reasoning with incomplete specifications
- Algorithms to discover hidden behaviors of composed systems
- Algorithms, scripts, regression unit tests, and documentation that makes no reference to systems other than the unclassified non-militarily relevant target platform

5.3 TA3 Voice of the Offense

- Configuration attack graphs specific to unclassified non-militarily relevant target platforms
- Algorithms to derive attack paths from system compositional model
- Algorithms, scripts, regression unit tests, and documentation that makes no reference to systems other than the unclassified non-militarily relevant target platform

5.4 TA4 System 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 of the combined integrated solution
- Evaluation approaches for maximizing test coverage of unclassified non-militarily relevant target platforms