MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF, NATIONAL GUARD BUREAU
COMMANDERS OF THE COMBATANT COMMANDS
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: (U//FOUO) Commercial-Off-The-Shelf Unmanned Aircraft Systems Implementation Guidance

(U//FOUO) References: Deputy Secretary of Defense Memorandum on Unmanned Aerial Vehicle Systems Cybersecurity Vulnerabilities dated May 23, 2018

1. (U//FOUO) Purpose: The intent of this guidance is to provide the exception approval process for procuring or operating Commercial-Off-The-Shelf (COTS) Unmanned Aircraft Systems (UAS).

2. (U//FOUO) Authority: The Deputy Secretary of Defense suspended the purchase and operational use of COTS UAS, due to cyber security vulnerabilities. The Deputy Secretary of Defense has delegated approval authority for all exemptions to the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) and Department of Defense (DoD) Chief Information Officer (CIO).
3. (U//FOUO) **COTS Definition:**

a. (U//FOUO) All UAS systems that are sold in substantial quantity in the marketplace and are offered to the Government in the same form in which it is sold to non-government consumers. The UAS systems are commercially available to the public including domestic and foreign manufacturers.

b. (U//FOUO) All UAS that in original form were commercially available, but have been modified with different hardware, software, or payloads.

c. (U//FOUO) All UAS ground command and control elements to include smart phone or tablet with associated software and hardware.

4. (U//FOUO) **Exceptions:** The following UAS systems are not covered by this implementation guidance and do not require submission of an exemption request:

a. (U//FOUO) That is managed by a formal Program of Record under a Service level program office; and

b. (U//FOUO) Has an authority to operate with a cyber vulnerability assessment.

5. (U//FOUO) **Exemptions:** All procurements and use requests for exemptions require prior approval and will be considered on a case-by-case basis for the following activities:

a. (U//FOUO) Critical operations with no alternative solution,

b. (U//FOUO) Counter-UAS surrogate testing and training, or

c. (U//FOUO) Intelligence and Information warfare testing, analysis, and training.

6. (U//FOUO) **Exemption Process:** The exemption for procurement and use of any COTS UAS or associated equipment (regardless of dollar value) must be approved. The exemption approval process is as follows:

a. (U//FOUO) All exception requests shall be handled by a single Service, Combatant Command (COCOM), or Agency Point of Contact (POC).

b. (U//FOUO) The Service, COCOM, or Agency POC will obtain written endorsement from the Component Head that includes a clear impact statement, rationale, technical information, and technical POC that should be addressed to the USD(A&S) and DoD CIO.

c. (U//FOUO) USD(A&S) and DoD CIO will evaluate the exemption request and render a decision.

7. (U//FOUO) **Technical Information Required:**
a. (U//FOUO) For unmodified COTS UAS using factory firmware, datalinks, and RC controllers provide the UAS make, UAS model, ground control station and software, payload make, payload model, and software.

b. (U//FOUO) For modified COTS UAS provide the name of system, model, hardware configuration, software configuration, network connections, data links, autopilots, network connectivity, ground controller, ground control software, payloads, payload data networks, and air-worthiness certification.

c. (U//FOUO) Location of use, time of use, airspace, operator, certificate of authorization (COA) and cybersecurity risk assessment.

d. (U//FOUO) Mitigation solutions to include hardware and software, Cyber Security vulnerability verification and validation, and results of a risk management decision by an authorizing official if one exists. Mitigation solutions should be in compliance with applicable DoD UAS cybersecurity policy such as 8500.01, Risk Management Framework, and DoDI S-4660.01, Encryption of Imagery Transmitted by Airborne Systems and Unmanned Aircraft Control Communications.

8. (U//FOUO) Clarification. This Directive includes all:

a. (U//FOUO) Government-owned COTS UAS unless excepted under paragraph 4 above,

b. (U//FOUO) Contractor-owned COTS UAS operated by or in support of Government operations or testing, and

c. (U//FOUO) COTS UAS being operated on DoD installations.

(U//FOUO) The technical POC for this implementation guidance is Mr. Brent Ingraham, OUSD(A&S), Tactical Warfare Systems, at Brent.G.Ingraham.civ@mail.mil or 703-693-9141.

Dana Deasy
Department of Defense
Chief Information Officer

Ellen M. Lord
Under Secretary of Defense for Acquisition and Sustainment