Counter-small Unmanned Aircraft Systems (C-sUAS)

Industry Day

AFRL/RIGD, 16 Dec 2019

Lt Col Bryan Fram, AFRL Deputy C-sUAS Lead

Brendon Poland, AFRL/RI, C-sUAS Lead Program Manager/Engineer

Donna Toole, AFRL/RI, C-sUAS IDIQ Acquisition/Program Manager

Terrence Lipinski, AFRL/RI, Contracting Officer

Agenda

- 0800-0900 Sign In
- 0900-0910 Intro/Acquisition Background -- Donna Toole
- 0910-0930 AFRL C-UAS Overview -- Lt Col Fram
- 0930-1030 C-sUAS Technology Areas -- Brendon Poland
- 1030-1100 Q&A

Lunch Break

- 1200 Small Business Break-out Sessions/15 mins blocks
- 1200-1600 Industry Networking (Auditorium)

Purpose

- General Session: Provide interested parties an overview of AFRL's role in C-UAS and the scope of the Counter small Unmanned Aircraft Systems (C-sUAS) Program
    - Overview of where we are going
    - Overview of current systems
    - Technical deep dive
    - Open forum for Q&A
    - Opportunity to meet with potential teaming partners
- Afternoon: One-on-One Sessions
    - Scheduled for 15 mins max
    - **AFRL is not requesting, nor will accept any marketing material**

Ground Rules

No audio or video recording is permitted.

- For questions that are not answered today you can submit them NLT 12 pm EST on 20 Dec 2019 to the following email addresses:

  terrence.lipinski@us.af.mil

  matthew.zawisza@us.af.mil

- AFRL will publish responses to all relevant questions from the presentations or one-on-ones, and will provide answers through beta.SAM.gov

Acquisition Team

- AFRL Deputy C-sUAS Lead – Lt Col Bryan Fram
- AFRL C-sUAS Tech Integration Lead – Phil Zaleski
- AFRL/RI, C-sUAS Lead Program Manager/Engineer – Brendon Poland
- AFRL/RI, C-sUAS IDIQ Acquisition Lead/Program Manager – Donna Toole
- AFRL/RI, Contracting Officer – Terrence Lipinski
- AFRL/RI, Contract Specialist – Matthew Zawisza

Acquisition Overview

Estimated IDIQ Labor Scope:

- Approximately 3.4M hours

Period of Performance:

- Anticipated Ordering Period: 72 Months
- R&D Task Orders (TOs) will be completed within 24 months after the ordering period ends

- Data Rights: Unlimited Rights desired
- Deliverable: C-sUAS fieldable prototypes
- Highest Security Classification: TS/SCI
- Export Control
- Travel: CONUS and OCONUS

Program History

- FA8750-16-C-0206, PAR Tech: Aerial Layer to a Cyber City (ALCC)
- FA8650-16-C-9205, TSC: Support Jammer Cueing (SJC) Rapid Reaction Technologies & Systems (RRTAS)
- FA8750-16-C-0293, AX Enterprize: Collaborative Low-Altitude UAS Integration Effort (CLUE)
- FA8650-17-C-9205 (SBIR II), Black River Systems: CUAS Open Systems Architecture (COSA)
- FA8650-17-C-9206 (SBIR II), DZYNE: Counter Unmanned Rapid Engagement Systems (CURES)
- FA8650-17-C-9207 (SBIR II), Sarcos: Small Drone Defeat System (S2DS)
- FA8650-17-C-9208 (SBIR II), Fortem: Mitigation of Small Unmanned Aircraft Systems
- FA8750-17-S-7001: Cyber Asymmetric Force Applications for UAS
- FA8750-17-C-0196, Raytheon: Vulnerability Analysis & Exploitation
- FA8750-17-C-0190, Steven Institute Contract: Acoustic Methods for UAS Detection, Tracking and Localization
- FA8750-17-C-0197, Black River Systems: Unmanned Aircraft Systems Asymmetric Cyber Applications (UASACA)
- FA8750-18-C-0041, KRI/Northeastern University: Unmanned Aerial Systems (UAS) Detection and Counter UAS R&D
- FA8750-19-C-0040 (SBIR III) Black River Systems: Operational Counter-sUAS Open Systems Architecture (OCOSA)

C-sUAS Technical Read Library

- Available now

- The library contains technical data subject to export control

- Potential Offerors who wish to gain access will be required to sign a Non-Disclosure Agreement (NDA), as well as furnish a copy of their company's DD Form 2345 - Militarily Critical Technical Data Agreement along with a letter from their Data Custodian designated on that form authorizing access by whomever will be reviewing the library. If interested in access to the technical library please contact Donna Toole by email at Donna.Toole.1@us.af.mil.

Acquisition Milestones

Milestone	Date
• Pre-Solicitation Notice	Nov 2019
• Tech Read Library (available)	
• Industry Day	Dec 2019
• RFP Release	Feb 2020
• Proposals Due	Mar 2020
• Contract Award	Sep 2020

- Note: Basic IDIQ to be awarded in conjunction with initial order

AFRL Counter UAS Overview

Lt. Col Fram

COTS C-sUAS Threat

- **Incredible Commercial Proliferation**
  - **New DJI Drone Every 3 Months**
  - **Autopilot Augmented and Silent Flight**
  - **Constantly Facing New Threat**
  - **US and Allied Forces At-Risk**

A drone sighting shut down Heathrow Airport, just weeks after a similar episode at London's Gatwick Airport. // Matt Dunham/AP

Who Keeps Buzzing London's Airports With Drones?

FEARGUS O'SULLIVAN JAN 9, 2019

Heathrow Airport was briefly shut down after a drone sighting, and Gatwick Airport endured three days of drone-related security delays.

WorldViews

The Kalashnikov assault rifle changed the world. Now there's a Kalashnikov kamikaze drone.

WORLD NEWS

A swarm of armed drones attacked a Russian military base in Syria

- Thirteen bomb-laden drones attacked two Russian military bases
- The attackers are unknown but Russia blames Syrian rebels backed by Turkey
- Pictures of one drone suggest a low-tech attack

David Reid | @cnbcdavy

Published 5:51 AM ET Thu, 11 Jan 2018 | Updated 9:10 AM ET Thu, 11 Jan 2018

CNBC

AFRL Investment Areas

Command and Control

- Modeling and Simulation
- Artificial Intelligence
- Human/Machine Teaming
- Engagement Automation

Detect → Track → Identify → Defeat

- Radar
- Lidar
- Acoustics
- Passive RF
- Electro Optical
- MASINT

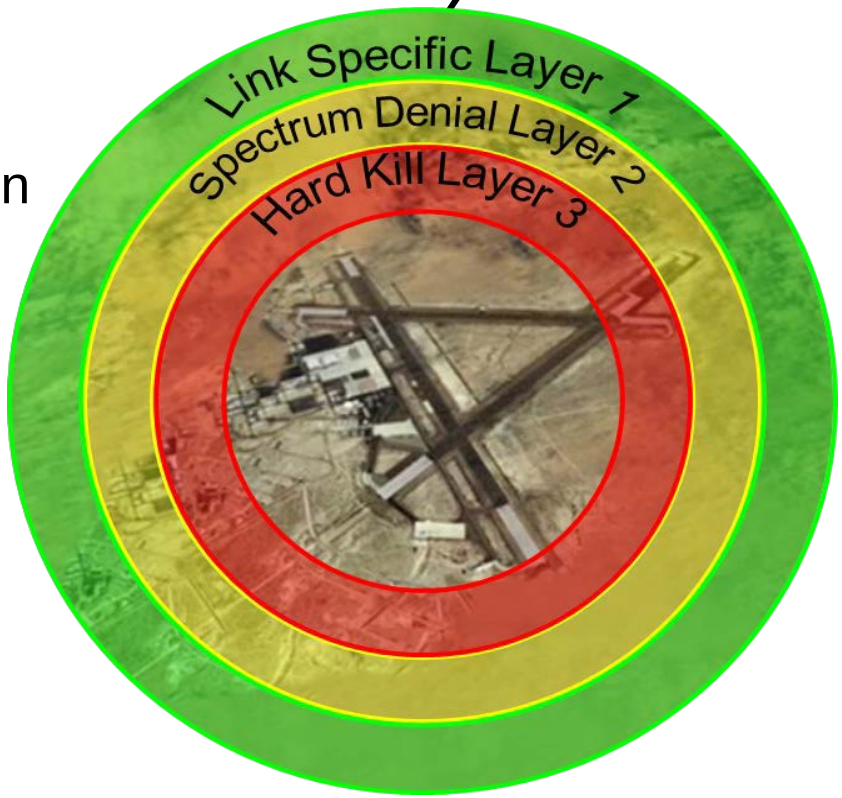
- Sensor Fusion
- Elucidation of Intent

- Interceptors
- Cyber / EW
- Directed Energy

Counter Small UAS Vision

Threat UAS

- Provide Options For Defensive Depth
- No “One Size Fits All” Solution
- Cost Effective
- Minimize Operator Cognitive Burden
- Open Source Solutions
- C2 Enhances Decisions On Short Timescales
- Integrate into Air Base Air Defense
- Industry Is A Critical Partner
- Extensibility to Group 3+



Can’t Wait For Crisis To Take Action On Counter-sUAS

C-UAS Technology Areas

Brendon Poland

Technical Objectives

1. Equip the US government with technical tools to combat the full spectrum of threats
2. Partner with industry to bring this technology to bear at wartime speed
3. Demand near symmetry to our costs and timelines in comparison to the threat
4. Balance “Cost Speed Quality” paradigm on a task by task basis

Technology development strategy

- Agile development of C-sUAS prototypes and capabilities that fill technology gaps across the entire C-sUAS kill-chain
  - Leverage existing and enabling technology to focus teams on non-realized capabilities
  - Layers of complementary and efficiently paired technology
  - Quickly assemble new teams with new ideas to tackle hard problems
  - Complementary Gov and contractor engineering teams
- Early experimentation and validation in near operational environments
  - Our DoD facilities are our test sites
  - Our Security Forces, Police and Defenders are our customers
- An Acquisition that can move tech from basic research all the way to fielded systems due to proof of tech utility in operational environments

Technical Focus Areas

- EW Enabled cyberspace countermeasures (CM)
- Low collateral damage (CD) Electronic Attack/CM
- C-sUAS operations in RF/Cyberspace contested environment
- Defensive Cyber Space Operation (DCO)
- Offensive Cyberspace Operations (OCO)
- Cyberspace C2
- Cyberspace Intelligence, Surveillance, and Reconnaissance (ISR)
- Automation and Autonomy of C2 systems
- Multi-domain C2 (MDC2)
- Airspace Coordination Measures (ACM)/Air Traffic Control (ATC)
- Unmanned Traffic Management (UTM) Systems
- Blue Force Interceptors
- Airborne C-sUAS C4ISR
- Directed Energy Weapon development and integration
- Sensor development and integration
- Tactical and Strategic tipping and cueing
- Signature and Effects Library

DIVERSE PROGRAM REQUIRING A BROAD SET OF SKILLS

Programs and Systems

- Mitigation of Unmanned Aircraft Systems (MUAS) Program
  - Cyber, Multi-Modality C2, Sensor exploitation
- Ninja System
- Guardian System
- Counter Autonomous Air (CAA) Program
  - C2 Automation, Swarm on Swarm operations, Counter Swarm capabilities

Summary

- **Technical Objectives**
  1. Equip the US government with technical tools to combat the full spectrum of threats
  2. Partner with industry to bring this technology to bear at wartime speed
  3. Demand near symmetry to our costs and timelines in comparison to the threat
  4. Balance “Cost Speed Quality” paradigm on a task by task basis
- **Technical Development Strategy**
  1. Agile Development
  2. Early Experimentation and Operational Evaluations
  3. End to End RDT&E (No Valley of Death)
- **Tech Areas**
  1. EW to Cyber
  2. Autonomous Command and Control
  3. Sensor Exploitation and integration
  4. Interceptors to Directed Energy

Questions?