Space Command and Control System (Space C2)

The Space Command and Control (Space C2) program continues to progress toward delivery of capabilities that will allow for the retirement of aging Space Defense Operations Center (SPADOC) infrastructure. In June 2023, DOT&E published a cyber survivability report on Warp Core, Space C2's Data-as-a-Service capability, finding it to be resilient to nascent-level cyber threat actors and to have appropriate defensive response capabilities to address emulated cyber threats on some classification domains. Operational testing of the Advanced Tracking and Launch Analysis System (ATLAS), Space C2's primary Space Domain Awareness Command and Control (SDA C2) capability, which had been planned for FY23, was slowed by delayed capability delivery, system stability problems, lack of trained operators, and non-operationally representative test environments.

SYSTEM DESCRIPTION

The Space C2 system uses a common commercially supported platform to access data and services for user applications that enable command and control operations. Space C2 uses a hybrid cloud, as well as hardware at operations centers, for resiliency and accessibility, and to enable multi-domain operations that are integrated with classified mission partner capabilities.

System capabilities fall into three updated mission-focused product portfolios:

- Space Defense focuses on providing the U.S. Space Command's Joint Task Force – Space Defense (JTF-SD) with operational command and control capability and supporting battle management services for the integration of new and legacy systems to address critical mission needs.
- SDA C2 focuses on developing the next generation of SDA capabilities for the Combined Force Space Component Commander, Space Delta 2, and users at the 18th Space Defense Squadron (18 SDS) and JTF-SD. This portfolio includes ATLAS.
- Cross-Mission Data focuses on providing an enterprise data integration capability that spans the U.S. Space Force (USSF) and DoD user base. This portfolio includes Warp Core.

The system has its own continuous integration/continuous deployment (CI/CD) pipeline, known as Kobayashi Maru, for capability and application development. Space C2's development efforts are primarily focused on delivering the capabilities that will allow for the retirement of the outdated SPADOC.

MISSION

USSF Guardians will use Space C2 to provide a wide range of space defense, SDA C2, and cross-mission data capabilities to facilitate timely, quality battlespace decisions by DoD and mission partners at multiple classification levels. Those capabilities include infrastructure, data and enterprise services, and mission applications to enable responsive, resilient operational-level command and control capabilities for the National Space Defense Center, the Combined Space Operations Center, 18 SDS, and other command and control centers.

PROGRAM

The Space C2 program was initiated as a Development, Security, and Operations (DevSecOps) pathfinder in 2019, and is continuing to seek designation as a software acquisition pathway (Execution Phase) program. That decision, which had been anticipated in December 2022, is now not expected until 1QFY24 due to delays in closing acquisition decision memorandum-mandated actions related to program documentation. The program, which has been on the DOT&E oversight list since FY19, formally submitted its test and evaluation strategy (TES) in 1QFY23. DOT&E approved the TES in 2QFY23.

In FY22, the Space C2 program restructured its capability development efforts to focus on the near-term challenge of retiring outdated SPADOC infrastructure. The restructure was intended to accelerate delivery of ATLAS capabilities to allow for the decommissioning of SPADOC, while deemphasizing the delivery of non-critical applications. In FY23, the foundational capabilities required to allow for the retirement of SPADOC infrastructure were the focus of product developers. While progress has been made due to the program restructure, product development has been slower than anticipated, and the projected date to decommission SPADOC continues to extend further to late FY24, a delay of more than two years from the original timeline.

The Space C2 program uses an integrated testing construct and has made significant efforts to define how it will accomplish that testing within USSF's new Integrated Test Force model. The program currently implements quarterly integrated testing events to assess SDA C2 capabilities. Despite those efforts, the program struggled to define incremental capability operational acceptance T&E goals and test methodology. To address those problems, USSF chartered the Space C2 Integrated Test Force in September 2023

to implement their vision for the Space Test Enterprise.

» MAJOR CONTRACTORS

Space C2 is comprised of a multitude of contracts and contractors developing capabilities, including:

- Parsons Corporation, Space Operations Division – Centreville, Virginia
- Omitron, Inc. – Colorado Springs, Colorado
- Tecolote Research, Inc. – Goleta, California
- Systems Planning and Analysis, Inc. – Alexandria, Virginia
- The Boeing Company – El Segundo, California
- General Dynamics Missions Systems – Fairfax, Virginia
- Lockheed Martin Corporation – King of Prussia, Pennsylvania
- Peraton, Inc. – Herndon, Virginia
- Palantir Technologies, Inc. – Denver, Colorado
- L3Harris Technologies, Inc. – Colorado Springs, Colorado
- Leidos Inc. – Reston, Virginia
- ManTech – Herndon, Virginia

TEST ADEQUACY

As discussed in the FY22 Annual Report, there were two Space C2 tests planned for early FY23. The first was the cyber adversarial assessment (AA) of Warp Core. The second was the operational utility assessment of ATLAS. USSF conducted the AA of Warp Core in accordance with a DOT&E-approved test plan in October 2022 at Vandenberg Space Force Base, California, with remote participation from McConnell AFB, Kansas, and Schriever Space Force Base, Colorado. The testing was observed by DOT&E, and despite Air Force cyber Red Team limitations, was adequate for DOT&E to assess Warp Core's cyber survivability. Both the Secret and Top Secret capabilities of Warp Core were tested, but activities focused on the Secret capability of Warp Core due to lack of Red Team preparation to assess the Top Secret capability. The AA demonstrated cross-domain solution functionality but did not assess the cyber survivability of the Warp Core cross-domain solution. Additionally, the CI/CD pipeline responsible for developing the applications that reside on Warp Core was also not evaluated for cyber survivability.

While integrated test events for ATLAS occurred in FY23, they did not produce operationally relevant data and cannot be used to meet operational test needs, primarily due to delayed capability delivery, system stability problems, a lack of trained operators, and non-operationally representative test environments. ATLAS operational testing is intended to be phased product release testing, aligned with program increment development timelines (approximately quarterly), executing as integrated tests known as SDA capability integrated tests (SCITs). SCITs are intended to produce usable data for both developmental and operational testing communities; however, the four SCITs conducted in FY23 produced little relevant operational test data. Test activities were primarily useful to the contractor testers, government-led developmental testers, and numerical validation analysts responsible for ensuring ATLAS accuracy meets the minimum legacy program standards.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

No data to inform an assessment of operational effectiveness or suitability was collected for the Space C2 program in FY23.

» SURVIVABILITY

Warp Core is resilient to nascent-level cyber threat actors and has appropriate defensive response capabilities to address the emulated cyber threats on some security domains. The Red Team could not penetrate the Warp Core infrastructure and could not generate any cyber effects against Warp Core or its end users by using nascent-level techniques in any of the postures. Since the Red Team was not able to compromise the system or produce any effects, they requested that the program office and the system developer (Palantir Technologies, Inc.) fabricate a cyber compromise of system data in order to capture end-user responses and mission effects during the test. Those fabricated data scenarios resulted

in successful detection of modified data by end-users, leading them to employ appropriate actions to notify supervisors of the discovery and proceed with proper prevention/mitigation procedures.

Other survivability findings dealt with known configuration issues for classified security domains and were not directly attributable to Warp Core.

Full details are included in the DOT&E Space C2 Warp Core Cyber Survivability Report and classified annex published in June 2023.

RECOMMENDATIONS

The USSF should:

1. Ensure the organizations responsible for future cyber survivability assessments of Space C2 capabilities are appropriately prepared and resourced to provide threat-representative cyber activities, including those related to commercial cloud assessments.
2. Perform additional government-led cyber survivability testing of Space C2 capabilities, including the CI/CD pipeline and cross-domain solutions, as part of major capability releases, once all relevant external users, data feeds, and operational applications are finalized across each applicable security domain.
3. Continue to refine the Integrated Test Force construct to define common T&E goals and methodology across all USSF programs in order to satisfy the equities of all T&E stakeholders.
4. Continue focused efforts on development and adequate operational testing of SDA capabilities required to complete the SPADOC decommissioning.
5. Continue to fund the assignment of cyber defenders for Space C2-related capabilities.