

**CSIAC TECHNICAL INQUIRY (TI) RESPONSE REPORT**

Overarching Wireless Technology Program for Flight Lines in the U.S. Air Force

**Report Number:**

CSIAC-BCO-2022-247

**Completed September 2022**

**CSIAC** is a Department of Defense Information Analysis Center

**Main OFFICE**

4695 Millennium Drive

Belcamp, MD 21017-1505

Office: 443-360-4600

**REPORT PREPARED BY:**

Olutoye Sekiteri

Office: CSIAC

Information contained in this report does not constitute endorsement by the U.S. Department of Defense or any nonfederal entity or technology sponsored by a nonfederal entity.

CSIAC is sponsored by the Defense Technical Information Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering. CSIAC is operated by the SURVICE Engineering Company.

|  |  |
| --- | --- |
| REPORT DOCUMENTATION PAGE | Form ApprovedOMB No. 0704-0188 |
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering, and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.** |
| 1. REPORT DATE *(DD-MM-YYYY)*01-09-2022 | 2. REPORT TYPETechnical Research Report | 3. DATES COVERED *(From – To)* |
| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBERFA8075-21-D-0001 |
| Overarching Wireless Technology Program for Flight Lines in the U.S Air Force | 5b. GRANT NUMBER |
|  | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| Olutoye Sekiteri | 5e. TASK NUMBER |
|  | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)AND ADDRESS(ES) | 8. PERFORMING ORGANIZATION REPORTNUMBER |
| Cybersecurity & Information Systems Information Analysis Center (CSIAC)SURVICE Engineering Company4695 Millennium DriveBelcamp, MD 21017-1505 |  |  |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR’S ACRONYM(S) |
|  |  |  |
| Defense Technical Information Center (DTIC) |  |  |
| 8725 John J. Kingman Road |  | 11. SPONSOR/MONITOR’S REPORT |
| Fort Belvoir, VA 22060-6218 |  |  NUMBER(S) |
|  |  | CSIAC-BCO-2022-247 |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT**DISTRIBUTION A.** Approved for public release: distribution unlimited. |
| 13. SUPPLEMENTARY NOTES |
| 14. ABSTRACTThe Cybersecurity & Information Systems Information Analysis Center (CSIAC) was tasked with researching and identifying an all-encompassing wireless technology program for wireless communications on flight lines used by the United States Air Force (USAF). CSIAC identified wireless standards provided by the U.S. Department of Defense (DoD) that should be followed by all DoD programs, employees, and contractors. CSIAC also identified various modern wireless technologies used to improve wireless connection on flight lines and hangars and standard processes used to implement these wireless technologies effectively and efficiently. Wireless communication technology is especially important to supporting flight line operations and maintenance workflows. Improving these technologies could improve the productivity and efficiency of operations personnel. Throughout the USAF, implementing new wireless technologies varies base by base, as the infrastructure is designed specifically to each base’s needs. |
| 15. SUBJECT TERMSAir Force, wireless technology, wireless standards, mesh networks, CBRS, flight lines |
| 16. SECURITY CLASSIFICATION OF: U | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSONTed Welsh, CSIAC Director |
| a. REPORTU | b. ABSTRACTU | c. THIS PAGEU | UU |  | 19b. TELEPHONE NUMBER *(include area code)*443-360-4600 |
|   | Standard Form 298 (Rev. 8-98)Prescribed by ANSI Std. Z39.18 |

# ABOUT DTIC AND CSIAC

The Defense Technical Information Center (DTIC) preserves, curates, and shares knowledge from the U.S. Department of Defense’s (DoD's) annual multibillion dollar investment in science and technology, multiplying the value and accelerating capability to the Warfighter. DTIC amplifies this investment by collecting information and enhancing the digital search, analysis, and collaboration tools that make information widely available to decision makers, researchers, engineers, and scientists across the Department.

DTIC sponsors the DoD Information Analysis Centers (IACs), which provide critical, flexible, and cutting-edge research and analysis to produce relevant and reusable scientific and technical information for acquisition program managers, DoD laboratories, Program Executive Offices, and Combatant Commands. The IACs are staffed by, or have access to, hundreds of scientists, engineers, and information specialists who provide research and analysis to customers with diverse, complex, and challenging requirements.

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) is a DoD IAC sponsored by DTIC to provide expertise in four technical focus areas: cybersecurity; knowledge management & information sharing; modeling & simulation; and software data & analysis. CSIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001.

A chief service of the DoD IACs is free technical inquiry (TI) research, limited to 4 research hours per inquiry. This TI response report summarizes the research findings of one such inquiry jointly conducted by CSIAC.

# ABSTRACT

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) was tasked with researching and identifying an all-encompassing wireless technology program for wireless communications on flight lines used by the United States Air Force (USAF). CSIAC identified wireless standards provided by the U.S. Department of Defense (DoD) that should be followed by all DoD programs, employees, and contractors. CSIAC also identified various modern wireless technologies used to improve wireless connection on flight lines and hangars and standard processes used to implement these wireless technologies effectively and efficiently. Wireless communication technology is especially important to supporting flight line operations and maintenance workflows. Improving these technologies could improve the productivity and efficiency of operations personnel. Throughout the USAF, implementing new wireless technologies varies base by base, as the infrastructure is designed specifically to each base’s needs.

**Contents**

[ABOUT DTIC AND CSIAC i](#_Toc118901814)

[ABSTRACT ii](#_Toc118901815)

[1.0 TI Request 1](#_Toc118901816)

[1.1 Inquiry 1](#_Toc118901817)

[1.2 Description 1](#_Toc118901818)

[2.0 TI Response 1](#_Toc118901819)

[2.1 Notable Wireless Standards 1](#_Toc118901820)

[2.1.1 BITI 1](#_Toc118901821)

[2.1.2 FIPS 140-2 2](#_Toc118901822)

[2.1.3 FIPS 140-3 2](#_Toc118901823)

[2.1.4 NIST SP 800-153 2](#_Toc118901824)

[2.1.5 DoD Directive 8100.02 2](#_Toc118901825)

[2.2 WIRELESS Technologies and Implementation 3](#_Toc118901826)

[REFERENCES 5](#_Toc118901827)

# 1.0 TI Request

## 1.1 Inquiry

Is there an overarching Wi-Fi program for the United States Air Force (USAF)?

## 1.2 Description

The Cybersecurity and Information Systems Information Analysis Center (CSIAC) was asked if the USAF had any specific guidance on standard, approved wireless technologies. The inquirer is working on prototyping software and tools that can help advance capabilities on the flight line; however, these devices need the correct connectivity to function properly in a flight line environment.

# 2.0 TI Response

## 2.1 Notable Wireless Standards

To have the correct wireless infrastructure and security posture, the wireless environment must comply with various standards provided by the U.S. Department of Defense (DoD). The USAF determined they need a wireless platform that could incorporate layer 2 encryption and wireless intrusion detection systems, support complex applications, and meet or exceed all DoD security standards [1]. Some notable wireless standards found are the Base Information Transport Infrastructure (BITI) wired/wireless program [2], the Federal Information Processing Standard (FIPS) 140-2 Certification [3], the Federal Information Processing Standard (FIPS) 140-3 Certification [4], the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-153 [5], and the requirements outlined in DoD Directive 8100.02 [6].

### 2.1.1 BITI

In 2009, the Combat Information Transport System program was restructured into two pre-Major Automated Information System components—Information Transport System (ITS) and Air Force Intranet. In 2012, the ITS program was renamed BITI, which included the wired and wireless components [2]. BITI wired provides the core Air Force network infrastructure for 178 fixed Air Force installations and geographically separated units. BITI wired capabilities encompass optical cable systems, digital voice/data/video systems, and allied support, resulting in high-speed packet switching and circuit transport of critical information among core buildings and mission areas on a base. Additionally, BITI wireless provides a robust and secure wireless infrastructure that incorporates high-availability and multitiered network connections at facilities requiring remote access, such as flight lines, hangars, medical facilities, and large storage areas.

### 2.1.2 FIPS 140-2

The FIPS 140-2 certification identifies the security requirements that should be fulfilled by a cryptographic module implemented within a security system protecting sensitive but unclassified information. FIPS 140-2 also provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification, cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility; self-tests; design assurance; and mitigation of other attacks [3].

### 2.1.3 FIPS 140-3

On 22 March 2019, the Secretary of Commerce approved [FIPS 140-3](https://csrc.nist.gov/publications/detail/fips/140/3/final), “**Security Requirements for Cryptographic Modules**,” which supersedes FIPS 140-2. This was [announced in the Federal Register](https://www.federalregister.gov/d/2019-08817) on 1 May 2019 and became effective 22 September 2019. FIPS 140-2 will run through 2026 [4].

The new standard introduces some significant changes. Rather than encompassing the module requirements directly, FIPS 140-3 references the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 19790:2012 security requirements. The testing for these requirements will be in accordance with ISO/IEC 24759:2017 security requirements. While there are few major technical requirement changes, the use of the ISO documents requires several procedural changes in the management and execution of the validation program and process [4].

### 2.1.4 NIST SP 800-153

NIST SP 800-153 provides organizations with recommendations for improving the security configuration and monitoring of their IEEE 802.11 wireless local area networks and devices connecting to those networks [5].

### 2.1.5 DoD Directive 8100.02

The purpose of DoD Directive 8100.02 is to establish policies and assign responsibilities for the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid; direct the development and use of a knowledge management process to promote the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout the DoD; and promote joint interoperability using open standards throughout the DoD for commercial wireless services, devices, and technological implementations [6].

Overall, these standards were created and put in place to ensure that wireless technologies are implemented and managed properly and can be secured properly.

## 2.2 WIRELESS Technologies and Implementation

There are four key reasons for problems that arise with wireless connectivity in hangars and flight lines:

1. There is such a large and vast amount of space in which a wireless signal must travel.
2. Many of the structures in these environments are created with metal, concrete, and other building materials which can block wireless signals.
3. There is a dynamic array of vehicles that can be present in a hangar or flight line at any given moment; these vehicles tend to also block wireless signals.
4. Enterprise/commercial-grade, wireless access points may perform well in an office setting but poor on flight lines.

When trying to advance the wireless capabilities of a wireless environment, there are very important steps that should be a part of every implementation effort. First, conduct a site survey of the wireless environment. Make sure to interview on-the-ground personnel about their daily workflows, when they access the wireless network, and where they see the most issues [7]. Then, measure the overall wireless coverage throughout the location. This includes measuring the average wireless signal strength, download speeds, upload speeds, and latency for every wireless access point. Next, based on the site-survey and measurements, create a wireless coverage model of the wireless environment needing improvement [8]. This wireless coverage model will be the roadmap to implement any new wireless technologies efficiently and cost effectively.

There are two major wireless technologies currently being implemented to improve wireless capabilities in hangars and flight lines throughout the USAF—mesh networks and citizens broadband radio service (CBRS)/private long-term evolution (LTE).

A mesh network is a network of devices or nodes connected directly and dynamically without a node taking priority over another. Each node connects to as many other nodes as possible and can dynamically change which node it connects to based on the wireless environment or scenario. For example, if a wireless access point is obstructed by a plane on the flight line while trying to connect to another node, it can redirect its connection to another unobstructed access point. Mesh networks allow organizations to efficiently route data from one user to another while maintaining a consistent connection throughout a wireless environment.

CBRS is a lightly licensed band that uses the 3550–3700-MHz band (3.5-GHz band) for shared commercial use. CBRS also features a dynamic spectrum access system which manages the allocation of frequencies in this shared range. CBRS uses a three-tiered access and authorization framework. Incumbent access users (Tier 1), which include authorized federal users within the 3550–3700-MHz range, receive protection against harmful interference from priority access licensees (PALs) and general authorized access (GAA) users. The priority access tier (Tier 2) consists of PALs that will be licensed on a county-by-county basis through competitive bidding. Each PAL consists of a 10-MHz channel within the 3550–3650-MHz band. PALs are 10-year renewable licenses and must protect and accept interference from incumbent access users but receive protection from GAA users. The GAA tier (Tier 3) is licensed by rule to permit open, flexible access to the band for the widest possible group of potential users. GAA users can operate throughout the 3550–3700-MHz band, must not cause harmful interference to incumbent access users or priority access licensees, and must accept interference from these users [9].

While the Citizens Broadband Radio Service can be used for 4G LTE, it is ideally suited to delivering fixed or mobile 5G new radio (5GNR). Specifically, CBRS can be employed by enterprise information technology providers to build out a private LTE network supporting large warehouse facilities, sports stadiums, and remote mines. CBRS can replace existing distributed antenna systems, providing high-speed data offload and in-building coverage. This will be particularly important when deploying 5GNR in the gigahertz spectrum, where CBRS can offset the significant signal degradation experienced when traversing general construction materials [9].

In the briefing provided by the Sierra Nevada Corporation, they discuss adding more access points to improve coverage and redundancy and utilizing directional antennas for access points. The briefing also mentions installing a wireless mesh network to extend connectivity range and utilizing a private LTE as a complimentary network to support backup communications. These infrastructure upgrades were critical to supporting the flight line of the future improvements at Homestead Air Reserve Base in Florida [8]. The SMS Data Products Group, Inc. (SMS) team boosted antenna strength to extend the range of the access port devices needed for better flight line coverage. They also created a network configuration designed to allow the addition of mobile access points to communicate as a mesh network. The Air Force technicians could place these mobile devices and obtain connections in previously inaccessible flight line spots, enhancing mission critical coverage [7].

The way improvements are implemented into wireless environments depends on the wireless coverage model of the environment and the information gathered from the site survey. Different wireless environments require different implementations for the varying workflows of the USAF.

# REFERENCES

[1] Aruba Networks. “United States Air Force Worldwide Network Takes To The Air.” <https://www.arubanetworks.com/assets/cs/CS_cits.pdf>, accessed 20 March 2013.

[2] U.S. Air Force Hanscom Air Force Base United States. “Base Information Transport Infrastructure Wired (BITI Wired).” <https://apps.dtic.mil/sti/citations/AD1019580>, accessed 1 March 2016.

[3] NIST. “FIPS 140-2 Security Requirements for Cryptographic Modules.” <https://doi.org/10.6028/NIST.FIPS.140-2>, accessed 25 May 2001.

[4] NIST. “FIPS 140-3 Transition Effort.” <https://csrc.nist.gov/projects/fips-140-3-transition-effort>, accessed 10 July 2019.

[5] NIST. “Guidelines for Securing Wireless Local Area Networks (WLANs).” <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf>, accessed 1 February 2012.

[6] U.S. DoD. “Department of Defense Directive 8100.02.” <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/810002p.pdf>, accessed 14 April 2004.

[7] SMS Data Product Group, Inc. “Flight Line Performance – Improving Critical, Wireless Communications.” <https://www.sms.com/blog/case_study/flight-line-connectivity/>, accessed 18 August 2022.

[8] Air Force Institute of Technology Wright-Patterson Air Force Base. “Best Wireless Technology for the Flight Line of the Future: A Multi-Criteria Decision Making and Utility Theory Analysis.” <https://apps.dtic.mil/sti/citations/AD1106273>, accessed 5 June 2020.

[9] Federal Communications Commission. “3.5 GHz Band Overview.” <https://www.fcc.gov/wireless/bureau-divisions/mobility-division/35-ghz-band/35-ghz-band-overview>, accessed 8 August 2022.