Space Systems Capabilities Brief.

ClearFocus® Technologies is an advanced cybersecurity company with a focus on cyber-physical systems in federal and DOD environments. We offer proven services assessing and securing aerospace systems from advanced threats who wish to hold US systems at risk. Space systems consist of three critical segments: space, ground, and user, and the security of each segment plays a pivotal role in the overall functionality and resiliency of aerospace systems. In the space segment, securing satellite systems is paramount, including telemetry and control for satellite operations. The ground segment involves ground control systems and commercial ground station services, such as AWS Ground Station, where cybersecurity measures are crucial to safeguard communication channels and data transmission. Additionally, cybersecurity for the user segment encompasses IT security to protect end-users interacting with aerospace systems, ensuring the confidentiality and integrity of user-related information.

NIST RMF/CYBER SECURITY FRAMEWORK

ClearFocus understands the unique challenges to protect systems operating in space and the ground and user segment systems that support space-based missions. We specialize in navigating the unique challenges associated with certifying space systems, evaluating impacts, and implementing security controls to guarantee the integrity and reliability of aerospace technologies. Our aerospace cybersecurity services are equipped to deliver comprehensive risk assessments through rigorous evaluations and testing, ensuring the robustness of space, ground, and user segments. We excel in identifying vulnerabilities and potential threats, providing clients with a clear understanding of their cybersecurity posture.

ClearFocus understands the unique challenges in accrediting and assessing space platforms, and the various guidelines including NISTIR 8270, NIST 800-53, and relevant Committee on National Security Systems and Intelligence Community Directive documents. Consequence-based cybersecurity evaluations are imperative components of aerospace cybersecurity. These evaluations go beyond identifying vulnerabilities and focus on assessing the potential impacts of cyber threats. By understanding the consequences of a security breach, aerospace organizations can prioritize their response efforts and allocate resources effectively to mitigate the most significant risks.

ClearFocus is currently an independent assessor for NASA Jet Proposal Laboratory and has assessed vulnerabilities of space hardware, both pre- and post-launch, which includes systems that reside in Low Earth Orbit (LEO) and destinations that include Mars and asteroids. Additionally, we have provided cybersecurity protections for satellite systems supporting sensitive military operations. From securing satellite communications to fortifying ground-based control systems, our experts leverage the latest technology and industry-leading practices to ensure space systems are secure. ClearFocus supports Space Systems for NASA, NOAA and other undisclosed clients.

CORPORATE PROFILE

Established in 2012

SBA Small Business and Certified HUBZone Company

DOD TS FCL

NAICS Codes: 541511, 541512, 541513, 541519, 541611

GSA Schedule 70 contract holder with all five Highly Adaptive Cybersecurity Services Special Item Number (HACS SIN) sub- categories

- High Value Assessments
- Risk & Vulnerability Assesments
- Cyber Hunt
- Incident Response
- Penetration Testing

PAST PERFORMANCE

USAID, U.S. Department of Homeland Security, DOE Office of Intelligence (DOE-IN), DOE-HQ, DOE Federal Energy Regulatory Commission (FERC), Sandia National Laboratories, U.S. Nuclear Regulatory Commission, Nevada National Security Site (NNSS), DHS, FBI, Bureau of Economic Analysis (BEA), NOAA, NASA, DOD, DISA, U.S. Air Force, USDA, DOJ, DOJ FBI, U.S. Courts, National Sciences Foundation, Selected Services System, U.S. Securities and Exchange Commission, Consumer Financial Protection Bureau, and the Library of Congress.

clearfocustech.com

305 Harrison Street SE, Suite 100B
Leesburg, VA 20175
Tel (703) 594-9033

GAS INTERNATIONAL ISO 9001:2015 REGISTERED COMPANY
GAS INTERNATIONAL ISO/IEC 20000:2018 REGISTERED COMPANY
GAS INTERNATIONAL ISO/IEC 27001:2022 REGISTERED COMPANY
SBA HUBZONE CERTIFIED
CMMI SVC | ML 2 APPRAISED Appraisal # 60954 | Exp. Oct 21, 2025
GSA IT Schedule 70 Contract Holder Contract GS-35F-444CA

PENETRATION TESTING AND RED TEAMING

Space systems pose a lucrative target for adversaries, and opportunities to fix or mitigate vulnerabilities are limited once systems begin their mission. Discovering and mitigating vulnerabilities before operations provides more options to mitigate vulnerabilities and introduces far less risk than once systems are in orbit. We offer penetration testing and red teaming services for all segments of space systems, particularly pre-launch. We can help implement and utilize existing modeling, simulation and flat-sat platforms to assess cybersecurity of systems. We understand the unique threat landscape which impacts ground control equipment as well as Radio Frequency (RF) uplink and downlink. We have experience leveraging software defined radios to emulate, capture, and interact with telemetry and control and are familiar with many space-based protocols, including a MIL-STD-1553, MIL-STD-188-165A, and a range of CCSDS standards. We will leverage our expertise to develop safe testing approaches which demonstrate actual threats and vulnerabilities against the system. Our assessments methodologies are grounded in threat intelligence and take a consequence-driven approach to identifying and mitigating attacks with the greatest potential impacts to the success of the mission.

HARDWARE AND EMBEDDED SYSTEMS SECURITY

Hardware and embedded systems security form a cornerstone of our expertise. We offer tailored solutions to fortify these critical components against emerging threats, including side-channel attacks and glitching attacks. Our services encompass the implementation of secure design principles and robust cryptographic measures to safeguard aerospace infrastructure. ClearFocus, leveraging its experience with Operational Technology (OT) environments, understands the vulnerabilities of space resident hardware and the RF communication from ground stations. We understand the different communication protocols and how to protect transmissions to space. We recognize the various mission constraints of weight, power, and link budgets which may limit options for cybersecurity controls. Our embedded systems process are designed to understand and assess systems, whether in early design phases and current operations, to identify potential risks and weaknesses across the systems. Examples may include unencrypted communication between components, such as SPI and serial communications, and potentials for compromised user payloads to gain access to control busses.

SECURITY OPERATIONS: MONITORING AND HUNT

Efficient threat hunting is essential for aerospace cybersecurity, especially in the context of satellite systems. Detecting nation-state adversaries requires a proactive approach, conducting thorough threat hunts on both space and ground segments. The goal is to identify and neutralize potential threats from sophisticated adversaries seeking to compromise satellite operations. This approach is crucial for maintaining the security and integrity of satellite systems against advanced cyber threats.

Our proficiency in security monitoring sets us apart. We employ advanced techniques to proactively identify and neutralize potential threats in aerospace systems, particularly in satellite operations. Our Security Operations Center (SOC) monitoring operates on our proven Threat Defense Life Cycle which drives continuous improvement beginning with a threat-informed, consequence-based approach to implement automated and orchestrated monitoring, analysis, and response actions.

We have operated multi-year pursuit programs searching for nation-state adversaries in support of the intelligence community and have helped develop and conduct assessments for the nuclear weapons programs. We bring the expertise and best practices from these, as well as current threat intelligence information, to our hunt process to focus on specific adversaries in context of the target system and understanding of the negative impacts the adversary wishes to inflict. We apply this to the complex ecosystem of systems necessary to support space missions across the space, ground, and user segments to provide focused, deeply technical, high-value hunts which can range from weeks to long-term engagements. We can help successfully navigate the challenges of authorities and access to data across organizational components to help ensure low-risk, high-confidence hunts inform the security posture and risk status of space systems.