Axient's Cyber Services: Protecting the Nation's Most Critical Systems to Enable Mission Success

Accelerating Possible by Ensuring Systems and Data are Secure & Mission Ready

Axient's Cybersecurity teams leverage proven best practices and proven methods coupled with industry leading tools to ensure the Nation's most critical systems and infrastructure are effectively hardened and data is secure from breach by our adversaries. Our trained and certified cybersecurity practitioners are leading the way in securing some of the nation's most critical defense and space systems. Our cyber subject matter experts perform all phases of system security engineering from developing cyber strategies and policy to hardening and testing systems according to NIST and other applicable regulations.

Cyber Policy Development

Axient relies on years of experience to create and refine cyber policies for our customers that ensure the highest practical level of security without obstructing the mission. We create and maintain program protection plans, cybersecurity strategies, software assurance plans, Clinger-Cohen Confirmation documentation, and all artifacts required to support the Risk Management Framework (RMF) process. Working closely with our customers to produce these documents we can ensure they provide the foundations for securing the program or mission without unnecessarily hindering the efforts of the warfighter or mission.

Independent Cybersecurity Vulnerability Assessments

Axient conducts detailed independent cybersecurity vulnerability assessments in accordance with NIST SP 800-53, NIST SP 800-30, FedRAMP, and all other applicable regulations. We utilize the latest automated and manual tools mandated by the Defense Information Systems Agency (DISA), including all relevant Security Technical Implementation Guides (STIG), Security Requirements Guides (SRG), automated Benchmark files, the Security Content Automation Protocol (SCAP) Compliance Checker (SCC), and the Assured Content Assessment Solution (ACAS).

Axient led the effort to achieve Authority to Operate (ATO) for Space Based Infrared Systems (SBIRS) Computer Enclaves (CE)

About Axient

With over 2,200 employees, Axient is headquartered in Huntsville, Alabama and has provided premier services and solutions to the Federal Government for more than three decades. Axient's customers include the U.S. Space Force, U.S. Air Force, U.S. Army, U.S. Navy, Missile Defense Agency, and NASA. Axient is certified in the following: ISO 9001:2015, AS9100 Rev D, CMMIDEV Maturity Level 3, and has a DCMA Purchasing System, DCMA Property System, and DCAA Accounting System.

AXIENT

System Cyber Requirements Development and Refinement

Axient partners with government programs and industry system design agents for defense and space systems to ensure cyber requirements are properly incorporated into the system development lifecycle. Defining cyber requirements prior to milestone A rather than bolting them on later enables our customers to field secure systems more quickly and cost effectively.

Axient leads all phases of Cybersecurity for US Naval Surface Fleet combat systems and connected elements.

Cyber Threat & Risk Analysis and Assessment

Axient's cybersecurity subject matter experts analyze the latest threat data collected by government intelligence as well as industry to determine the potential risk and impact to mission systems. Using a proven, documented, and repeatable approach we thoroughly review known and forecasted cyber threats, assess how they might adversely affect a system, and provide our customers with the distilled, prioritized, and timely data required to make informed decisions. Our teams routinely provide recommended courses of action and often lead the efforts to implement those actions to protect the systems and critical mission data at risk.

Cyber Analysis of Alternatives

With a confusing multitude of available COTS and GOTS cybersecurity products and tools to choose from, Axient helps our customers better understand these options and make the best choices for each system and scenario. Our teams analyze the alternatives for mission critical products such as cross domain solutions, intrusion detection and prevention systems, and firewalls to determine which option(s) best meet the unique requirements of a particular system or enclave. We ensure that a proposed solution can adequately secure the system without sacrificing data availability and throughput or adding preventable latency.

Cyber Integration and Alignment

Axient's cybersecurity engineers and analysts work across programs with all stakeholders to confirm that cyber requirements and system capabilities are properly aligned to promote the success of the overall mission. Working in close coordination with combat systems and individual elements ensures that cyber acquisition schedules and product selections will properly integrate to reduce long term cost and schedule and meet program milestones and deadlines.

Our Cyber Professionals are Trained and Certified

CompTIA Security+™ CERTIFIED

NQV

CISM

CISSP®