CYBERSECURITY

Secure, Reliable Services and Solutions for Cyberspace

Secure, reliable data access becomes more important every day. But with better access comes increased risk. The growth of e-commerce and the Internet has been accompanied by dramatic increases in intrusion and misuse. Federal and Department of Defense (DoD) organizations are responding by prioritizing electronic security and creating or accelerating security technology programs. However, technology alone cannot prevent computer attacks—a multifaceted solution that assures data security without interrupting critical data flow is needed. Hexagon US Federal has the dedicated, certified resources and experience to offer a proven, comprehensive cyber security solution that will help protect your systems, network resources, and mission-critical data.

Federal, DoD, and Department of the Navy (DoN) organizations continuously work to achieve and maintain information dominance by advancing technology and operational capabilities, such as open system architecture, web enablement, network-centric operations on the Global Information Grid (GIG), cloud computing, and more that introduce new cyber security challenges. When moving from traditional computing to new, more advanced computing it is vital that all systems and processes are evaluated prior to adoption to ensure that (1) they meet cyber security standards, regulations, guidelines, policies, and procedures and (2) all potential vulnerabilities and risks are addressed.

Experience & Certifications

Hexagon's Cyber Security Group is comprised of experienced IT-Certified security professionals (CISSP, CISA, CISMA, CPP) as well as certified IT product specialists experienced in the preparation, verification, and submission of DoD Information Assurance Certification and Accreditation Process (DIACAP)

THE CYBER SECURITY LIFE CYCLE

We offer cyber security solutions that meet your precise needs, regardless of your organization's size or mission. We approach cyber security as a cycle of continuous improvements to your system and network defenses, including risk review, policy development, solution implementation, administrative support, auditing, and certification and accreditation.

and Risk Management Framework (RMF) packages, supporting IA control artifacts, Certificate of Networthiness (CoN), Network Assessments, SIPRNET and NIPRNET certifications, Vulnerability Assessments, and Risk Mitigation. We have the experience and knowledge to help ensure your organization's success in complying with regulations, standards, and guidelines such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), U.S. Army Regulations AR 25-1 and AR 25-2, NIST, U.S. Navy DIACAP and RMF Guidelines, and more.

Our recent past Cyber Security experience with the DoD, military and U.S. federal agencies includes:

- Secure VOIP implementation for NAVSEA
- U.S. Army, Navy, Marines and Air Force vulnerability assessments and risk remediation using DISA STIG Checklists and support tools
- U.S. Army and Air Force CoN Process
- DoD, Intelligence Community (IC), and military engineering application program system lockdown, risk posture assessments, DIACAP, Certification and Accreditation, and RMF assessment and authorization
- NAVAIR engineering/logistics application Certification and Accreditation packages using DoD and DoN regulations with Navy Network Warfare Command
- NAVAIR program IAV process using IAVA/B/Ts and CTOs from the Joint Task Force – Global Network Operations (JTF-GNO) and Navy Online Compliance Reporting System (OCRS)

Proven Tools

Our wide array of proven, powerful tools includes:

- WebInspect
- Security Content Automation Protocol (SCAP)
- Assured Compliance Assessment Solutions (ACAS)
- STIG Viewer
- Comprehensive Checklists

Looking Ahead

DoD computer systems and networks face constant and increasingly sophisticated attempts to procure data and even wrest control from their owners, launched by domestic and foreign hackers. But many organizations continue to view network security as a single event on a "to-do" list or as a checklist of steps taken whenever something bad happens. In the face of increased threat levels and new kinds of attacks, a more consistent and vigilant approach is required.

With our cyber security experience and associated lessons learned from our work securing Navy, Marine Corps, Army, Air Force, and other DoD computing environments, we are strongly positioned to assist your organization with cyber security issues, the transition from DIACAP to RMF, and the implementation of new environments such as cloud-based computing systems and services. We support our customers with cyber security tools and certified security subject matter experts, and we use best security business practices throughout every phase of every project to manage, control, and improve risk posture.

Contact Us

Email: info@hexagonusfederal.com
Tel: +1 800 747 2232

hexagonusfederal.com

About Hexagon US Federal

Hexagon US Federal is an independent subsidiary for Hexagon's U.S. federal business. Hexagon US Federal provides mission-critical and business-critical solutions to governments and service providers. A global leader, proven innovator, and trusted partner, our software and industry expertise help improve the lives of millions of people through safer communities, better public services, and more reliable infrastructure. Visit hexagonusfederal.com.

Hexagon US Federal is part of **Hexagon** (Nasdaq Stockholm: HEXAB; hexagon.com), a leading global provider of information technologies that drive productivity and quality across geospatial and industrial enterprise applications.