Faced with today’s intensifying threat environment, where do you turn for cyber security answers you can trust? How do you keep pace with rapidly changing threats, technologies and requirements? How do you choose the best cyber defense? And once in place, how do you know it’s working – 24/7?

General Dynamics Information Technology helps you define your cyber security needs and provides the solutions to achieve them. As a leading cyber security integrator, we deliver agile, defense-in-depth solutions geared to your mission and enterprise needs. Our full life-cycle capabilities range from assessments and architectures to operational support to innovation. After decades of proven experience with the defense and intelligence communities, we know how to make cybersecurity work – reliably, repeatably, measurably and affordably.

Our cybersecurity solutions have defended the most mission-critical systems, including tactical, cross-domain, large-enterprise and national networks. We use leading edge technology to correlate information on millions of cyber events to identify critical actionable incidents. Currently, the company operates more than 20 security operations centers (SOCs) and 15 critical incident response teams (CIRTs) across government and industry. We also provide proven metrics to measure SOC performance. You know how well your cyber security operations are working and how best to improve them.

General Dynamics Information Technology defends our Nation’s critical cyber resources and networks.
Defending Military Enterprises Worldwide. General Dynamics Information Technology is the leading provider of cyber security solutions to the U.S. Air Force and the Air Force Information Management program, which protects USAF data networks through 16 cyber security gateways that form a security boundary to shield 105 bases worldwide. This effort includes the AFNet Increment 1 redesign of the USAF’s unclassified and classified network management and network defense architecture. Responding to an urgent operational need for Pacific Air Forces (PACAF), we designed and deployed the initial intrusion prevention system and a modernized security information and event management capability within a compressed timeline.

We provide complete cyber security support to U.S. Army posts worldwide, including operation and maintenance of Army SOCs serving entire theaters of operation and more than 500 successful C&A assessments. Our cyber security experts evaluate products for technology insertion and furnish penetration testing for state-of-the-art combat technologies. Our team integrated cyber security into all phases of the Pentagon Renovation program, a ten-year modernization of Pentagon tenant organizations to a fully secure enterprise IT environment. This included SOC development and advanced capabilities such as secure Voice over Internet Protocol (VoIP).

Since 2005, we have helped the Missile Defense Agency ensure the security of its information infrastructure, providing information assurance (IA) services and C&A to meet Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) requirements.

Cyber Defense for Homeland Security Enterprises. We operate and sustain U.S. Customs and Border Protection’s SOC 24/7, ensuring network and information security for more than 60,000 users. The SOC processes tens of millions of events per month, cutting through the noise to identify and handle about 175 actionable incidents. We build and manage the SOC for U.S. Citizenship and Immigration Services (USCIS), providing ITIL-based security management for 18,000 users at 250 offices throughout the world.

Working with the U.S. Coast Guard (USCG) Telecommunication and Information Systems Command, we support the design, security and implementation of all USCG enterprise IT, Windows-based systems. Operating the USCG CIRT, we support an enterprise with gateways that handle 15.3 million emails per month, 43,000 of which have infections or malicious payloads.

Supporting the Intelligence Community’s (IC) Global Mission. General Dynamics Information Technology meets the demanding requirements of the IC. We are building and operating a modernized enterprise IT infrastructure, which employs an integrated enterprise data center designed to ensure the highest levels of security in a virtualized, cloud computing environment.

High-Level Security and Privacy Requirements for Modern Healthcare. Federal health organizations and commercial payers rely on General Dynamics Information Technology for expert services in cyber security, IA, regulatory compliance and applications security management. Our C&A audits ensure compliance with key standards, including HIPAA, FISMA and the HITRUST Common Security Framework. Continuous monitoring and SOC services defend information networks and protect data privacy. Proven analysis and testing services and tools ensure the security of new applications and eHealth initiatives. Our secure data center in Maryland, designed to meet strict health industry requirements, provides managed hosting for applications and data warehousing.

Supporting Federal Civilian Employees. General Dynamics Information Technology develops and manages SOCs throughout federal civilian government. Serving 5,000 sites, these include SOCs for the U.S. Department of the Treasury, Internal Revenue Service and Food Safety Inspection Service.

Our cyber security and network operations services support organizations such as the FBI, Federal Energy Regulatory Commission, Veterans Affairs, National Archives and Records Administration, Federal Highway Commission and the International Trade Administration.

General Dynamics Information Technology is the prime contractor for the IRS’ IT Computer Security Incident Response Center, proactively protecting and responding to threats against the IRS’ vast financial records and network since 2006. For the Federal Aviation Administration, we support its migration to a modern, secure communications infrastructure, including enterprise SOC support.

The General Dynamics SOC. Serving tens of thousands of users, the General Dynamics SOC safeguards our federated enterprise environment, detecting and responding to threats against the company’s cyber infrastructure and against company and customer data. Across General Dynamics Information Technology, our COTS-based tools process more than 60 million security events each day. Innovative event correlation reduces these to fewer than 50 actionable incidents. Our SOC also serves as a proving ground for our customers’ new security technologies and processes.

Knowledge gained on major programs brings best practices to our customers.
General Dynamics Information Technology’s strengths and innovation protect critical networks that are part of your federal enterprise today – and lay the foundation for more resilient cyber defenses in the future.

Cyber Security’s Front Lines. Our expert workforce features hundreds of IA professionals with sweeping technical skills, in-depth training and industry-recognized certifications. Those serving the defense community typically have current DoD security clearances or higher. We are also one of the first companies to adopt DoD 8570.01 certifications for IA workforce improvement.

Innovation Reduces Risk. General Dynamics Information Technology drives innovations you won’t find anywhere else. Our Security Management Operations Approach (SOMA) provides a repeatable, prescriptive framework for implementing and managing an enterprise cyber security operations program. Incorporating ideas and best practices from the IT Information Library (ITIL), CMMI for Services and CERT’s Incident Management Capability Metric, SOMA helps ensure effective operations, continuing improvement and comprehensive performance measurement.

We Fill the Gaps. Our innovative products fill key gaps, providing capabilities that commercial tools may lack.

- **TruDetect: Network Intrusion Detection System (IDS).** TruDetect finds sophisticated threats that signature and behavioral based IDS’s miss.
- **Citadel Cyber Targeting and Analysis Tool.** Citadel creates models that help senior managers make smart decisions on complex, high priority operational programs.
- **Specialized Tools.** We provide proven assessment, C&A and policy automation tools, plus customized tools for network defense and analysis.
- **Security Vulnerability Management Tool (SVMT).** Developed for USCIS, SVMT automates the aggregation and filtering of vulnerabilities from 350 field offices, 100 information technology systems and 40 applications. SVMT was a key component in raising the USCIS’s FISMA score from a failing grade to an “A.”

Meeting Critical Standards. Through our extensive C&A experience, we help you meet the latest security and IA standards. These include FISMA, DIA CAP, NIST, ISO and NAICAP, as well as HIPAA, HITRUST and ISO 27799:2008 standards for healthcare. Our specialists monitor and work closely with government cyber security programs, regulatory agencies and standards organizations. We also help you develop continuous compliance monitoring to support timely, affordable audits, C&A and reporting.

Respond Agilely, Defend Globally. Reduce your risk in an uncertain world. With cyber security solutions from General Dynamics Information Technology, you will respond agilely to the threats ahead as you defend your enterprise network around the globe.

www.gdit.com