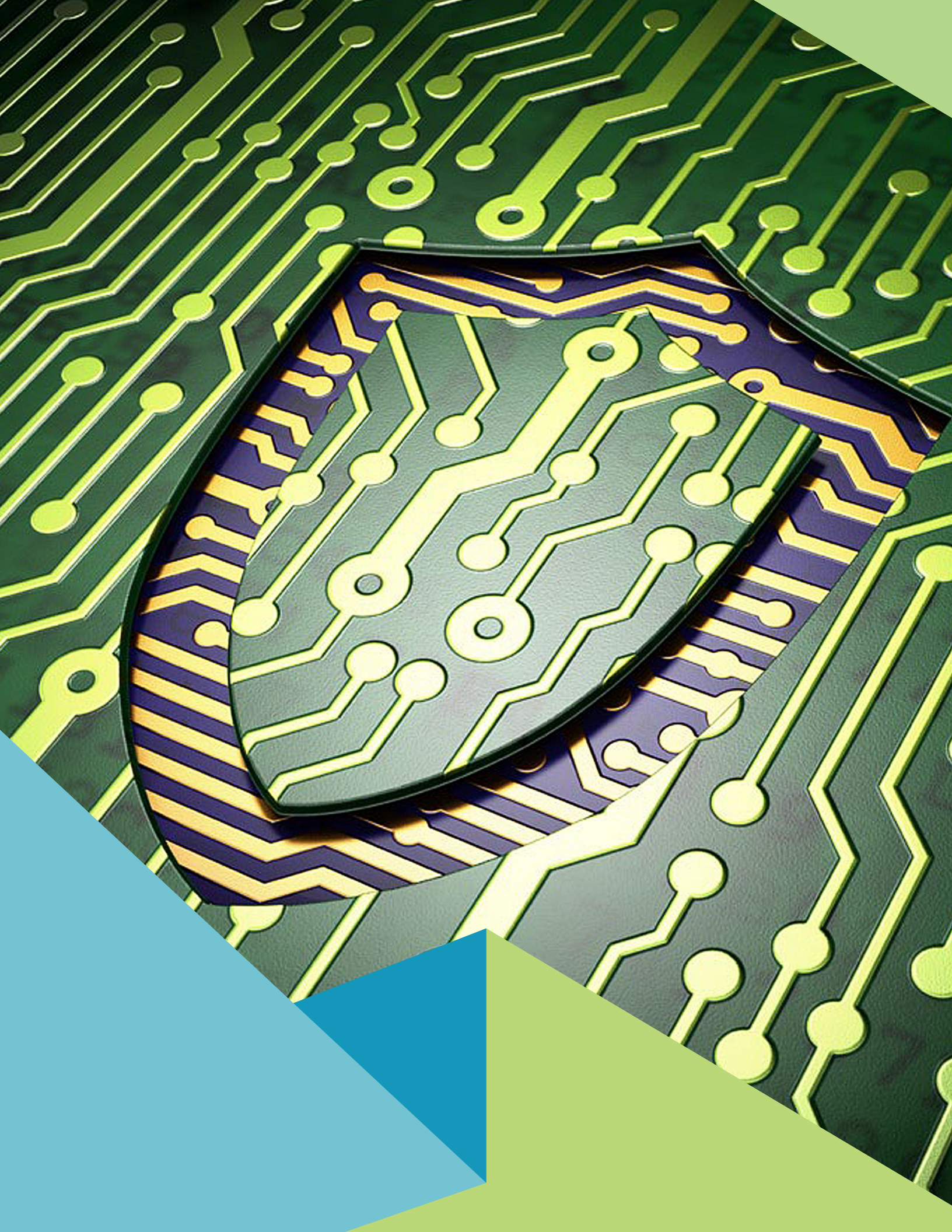
HEXAGON | US FEDERAL

CYBER SECURITY

Defending Your Valuable Information



CYBER SECURITY SOLUTIONS

In our increasingly competitive world, secure, reliable data access is more urgent than ever. But increased access comes with increased risk. The proliferation of e-commerce and the growth of the Internet have been accompanied by dramatic increases in unauthorized intrusion and network misuse. Federal agencies and businesses are responding by prioritizing electronic security and creating or accelerating security technology programs. However, technology alone cannot prevent cyber 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 you a proven, comprehensive cyber security solution that will help protect your systems, network resources, and mission-critical data.

HOW SECURE IS YOUR DATA?

Continuing research by the FBI and other law enforcement agencies confirms that the rate of data theft and other cyber crimes continues to rise, and the financial toll continues to mount. Highly publicized breaches of Personally Identifiable Information (PII), malware intrusions, and overt cyber attacks, including cyber attacks by terrorist hackers, are just the tip of the iceberg.

In fact, in 2012 the Identity Theft Resource Center (ITRC) reported that the business sector experienced over 35 percent of all publicly reported information security breaches. The number of reported breaches in 2012 was up 6.7 percent over 2011. The Internet Crime Complaint Center (IC³) stated that from January 1, 2011 through December 31, 2011, its website received 314,246 complaint submissions, a 3.4 percent increase over 2010. Financial losses linked to these complaints exceeded $485 million, nearly double the losses reported in 2008.

In 2008, the most frequently reported sources of cyber attack were malware infections (over 50 percent of organizations reporting cyber attacks reported malware infections) and insider abuse of network access (almost 45 percent). In 2010, reported malware infections rose to over 67 percent, but insider abuse fell, with 2010 levels only half those of 2008.

Phishing scams now represent the second most likely source of attack (almost 40 percent). Whether it stems from a virus written in a far-off country or a deception that fools employees in your organization, an attack on your information infrastructure could cost millions in lost sales, customers, trade secrets, and productivity.

HOW CAN YOU PROTECT YOUR DATA?

To prevent cyber crime, businesses and U.S. government organizations must develop plans to secure their information infrastructure. Cybersecurity surveys indicate that simply performing a risk assessment makes an organization four times more likely to detect identity theft. Moreover, government mandates such as the Health Insurance Portability and Accountability Act (HIPAA) for the healthcare industry, the Gramm-Leach-Bliley Act (GLBA) for the financial services industry, and the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) for the armed services, require baseline levels of cyber security to protect the privacy of consumers and U.S. citizens.

Unfortunately, many organizations don't know where to begin, and those that do lack resources, time, expertise, and knowledge. With our strong industry partnerships and our broad experience in systems integration, development, testing, training, and networking, Hexagon is uniquely suited to help you meet your information assurance (IA) needs.

I/Secure Life-Cycle IA Support

Computer systems and networks face constant and increasingly sophisticated attempts to procure data and even wrest control from their owners, launched by disgruntled employees, scammers, independent and state-sponsored hackers, and domestic and foreign terrorists. But many organizations 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 cyber crime, a more consistent and vigilant methodology is required.

Hexagon's I/Secure methodology approaches security as a continuous life cycle of cyber security improvements. Hexagon supports local security organizations in building an integrated, comprehensive approach guaranteed to increase security both immediately and in the future.

Hexagon also provides stand-alone, focused IA offerings such as risk and physical security assessments, certifications and accreditations, policy development and implementation, and privacy workshops to help our clients take the steps they need to defend their valuable information.

RISK REVIEW

Because networks frequently add new equipment, content, and users, you must regularly identify assets, assign value, and assess liabilities. You must consider questions such as:

- What data do you possess that you and others value?
- Whom do you consider unauthorized users?
- How might unauthorized users gain access to your IT assets, systems, networks, or data?
- What are the potential consequences and costs of a security breach?
- What types of protection will reduce risks to an acceptable level?

A LIFE CYCLE FOR SECURITY

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.

Hexagon helps establish procedures for conducting investigations of both your network and your physical environment, and we support you in assessing threat information, developing priorities, and working with team leaders to reduce risks. We can review your physical security and network and system architecture and make recommendations for improvements. Any organization using Web-based or information technologies will benefit from our support.

POLICY DEVELOPMENT

Every business and government organization has policies, procedures, advisories, standards, mandates, and regulations that address a range of security issues, from the physical to the virtual. Hexagon helps you review these documents, eliminate redundancy, and identify requirements for physical security, acceptable Internet use, messaging, network tools, and computer viruses. We'll help you define prevention, monitoring, and reaction procedures and plan policy education. By assigning responsibilities, you can ensure all policies and advisories are appropriately incorporated and enforced. Through continual review, you can simplify the dynamic policy development process.

Solution Implementation

Selecting technology tools is no easy task given the breadth of products available and the evolving capabilities needed to keep pace with changes in network speed and technologies. With broad experience in a wide array of multiplatform products and systems, Hexagon helps you evaluate available technologies such as cameras and sensors, databases, servers, network devices, intrusion detection systems, Internet scanners and firewalls, and detection software. We integrate and implement the infrastructure you need to meet your precise security needs.

An important step in implementing an IA program is to create a local response team that can deal firsthand with security issues and coordinate with regional or divisional organizations. Hexagon has extensive experience in establishing response team capability, with specific knowledge of how to approach network/system intrusion response. Hexagon also supports the implementation of management, response, mitigation, and reporting processes. We'll help you develop monitoring functions and implement daily, weekly, monthly, and quarterly tasks, as well as support metrics. With our help, you can balance your operational and security needs within realistic budgetary constraints.

Administrative Support

Once your security procedures are in place, Hexagon can support daily on-site administration to minimize risk. Using our proven systems engineering methodology, we help you manage your security processes, objectively review your results, and update your procedures and policies. We conduct training to educate users about acceptable use and conduct, introduce new procedures and policies, and increase security awareness.

We can also assist your IA officer in enforcing procedures, conducting incident investigations, and preparing reports for upper management or DoD submission. If an incident occurs, we help you minimize the impact of service disruption and information theft or loss for quick recovery.

Responding systematically with our solution, you can dramatically reduce the risk of recurrence.

Auditing, Certification & Accreditation

Successful security systems must be tested. That's why Hexagon helps you to assess the vulnerability of your system through intense penetration testing using the latest intrusion simulation methods.

We also participate in certification testing of all information systems due for accreditation or reaccreditation. We help you establish accreditation criteria and evaluation/certification processes and maintain a database of accreditation status and schedules.

CYBERSECURE BY DESIGN™

Our cyber security solutions provide dedicated, certified resources that will help you defend your systems against cyber crime. Because we build cyber security into every solution we provide, we help you secure your servers, data, applications, systems, and networks, and keep them secure. Our unique CyberSecureByDesign™ methodology incorporates input from customers, products, and regulations to produce a secure system that meets all your cyber security requirements.

CYBER SECURITY OFFERINGS

We bring over 35 years of cyber security experience to assist you with your IA needs. Our experienced, certified IA professionals and certified IT product specialists are experienced with an arsenal of tools that support

GET THE MOST FROM YOUR BUDGET

In today's environment of scarce funding and increased threat, you need the best cyber security solution for your dollar. Get the most from your budget with a security process that will shield your information assets and data well into the future. Add Hexagon s experience to your team today.

Proven SolutIon

The following is a list of Hexagon cyber security customers:

- Athens Limestone Hospital
- Centers for Disease Control
- Computer Associates
- Cryptek, Inc.
- Hexagon Australia
- Hexagon PPM
- NAVAIR JTDI
- New York City
- Palladia Systems, Inc.
- Publix Employees FCU
- UAB Health System
- Yuma Proving Grounds
- Lockheed Martin Svc, Inc.
- Children's Health System
- COSMIC
- EDS - Herndon
- Hexagon Canada
- State of Alabama
- NAVICP-Mech
- Omega
- U.S. Army AMCOM
- PEI Electronics, Inc. (DRS)
- Westar
- William Penn School District

your security assessment and implementation requirements, such as AppSecIn Appdetective, SpiDynamics WebInsptect, and eEye Retina. Throughout your project, we work with you using our CyberSecurebyDesign™ methodology, industry best practices, and extensive corporate knowledge to provide you with the ability to confidently monitor, manage, and improve your risk posture on an ongoing basis. Our Cyber Security offerings include:

- Security Application Assessment/ Certifications (for example, System and Application Certificate of Networthiness (Army), Standard Desktop and Server Configuration Certification Testing (Air Force))
- DIACAP (DoD Information Assurance Certification and Accreditation Process)
- On-Site and Off-Site IT Security Support Services
- System Hardening
- Physical Security Assessment
- Security Policy Development and Implementation
- Policy and Procedures Assessment
- Privacy and Public Law Strategy and Implementation
- Risk Assessment / Vulnerability Identification and Gap Analysis

CERTIFIED, EXPERIENCED PROFESSIONALS

Hexagon's cyber security engineers are experienced in supporting DoD, Federal, military, State, and international cyber security standards, regulations, and guidelines. Hexagon engineers also hold an array of certifications.

Cybersecurity Engineer Certifications

- Information Assurance Workforce–Technical (IAT) Levels I, II, and III
- Certified Information System Security Professional (CISSP)
- Certified Computer Examiner (CCE)
- Certified Information Security Auditor (CISA)
- Certified in Risk and Information System Control (CRISC)
- Fully Qualified Corporate Navy Validator
- NSA Infosec Assessment Methodology (IAM)
- GIAC Security Essentials Certification (GSEC)
- Microsoft Certified Professional (MCP)
- Microsoft Certified Solutions Expert (MCSE) 4.0
- Configuration Management II (CMII)
- ISC² Systems Security Certified Practitioner (SSCP)
- NSPE Professional Engineer (PE)
- DoD System Administrator
- DoD Network Administrator
- Information System Security Manager (ISSM)
- CompTIA Security+
- PMI Project Management Professional (PMP)

Hexagon engineers support numerous cyber security standards, regulations, and guidelines, including, but not limited to, the following:

- Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG)
- Risk Management Framework (RMF)
- Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)
- DoDD 8500.1, DoDI 8500.2, DoDI 8510.01
- Army Certificate of Networthiness (CON)
- Army Regulation (AR) 25-2
- National Institute of Standards and Technology (NIST)
- National Information Assurance Certification and Accreditation Process (NIACAP)
- Federal Information Security Management Act (FISMA)
- Federal Desktop Core Configuration (FDCC)
- Federal Energy Regulatory Commission (FERC)
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIPs 002–009)
- Federal Information Processing Standards (FIPS)
- ISO/IEC 27002 (Code of Practice for Information Security Management)
- ISO/IEC 15408 (Common Criteria)
- ISACA COBIT 5
- Information Technology Infrastructure Library (ITIL)

> Hexagon and the services they provided were instrumental in REMIS, HAPMIS and RECIS achieving favorable DIACAP and CoN status."

Rhonda Johnson, Program Management & Analyst
US Army Corps of Engineers Real Estate Systems National Center (RESNC)

> There is so much more illegal and unauthorized activity going on in cyberspace than corporations admit to their clients, stockholders, and business partners or report to law enforcement. Incidents are widespread, costly, and commonplace."

Patrice Rapalus, Director
Computer Security Institute

> I've been really impressed by the work done by Hexagon. Their knowledge and professionalism has been refreshing compared to other vendors we've worked with in the past. I would definitely recommend Hexagon to other companies seeking to outsource and hope to use them for future projects."

Karen Sullivan, Director of Information Technology
Publix Employees Federal Credit Union

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.

HEXAGON | US FEDERAL