



## Security Compliance

Effectively managing a secure infrastructure has always been a basic requirement for information technology departments. Today, however, managing the confidentiality, availability, and integrity of information assets for compliance is mandatory.

With businesses now relying on IT for a wider range of profitable activities, and with a growing risk environment, it is more important than ever to understand, characterize, document, and measure technology threats—and then institute well-accepted practices and protocols to mitigate them.

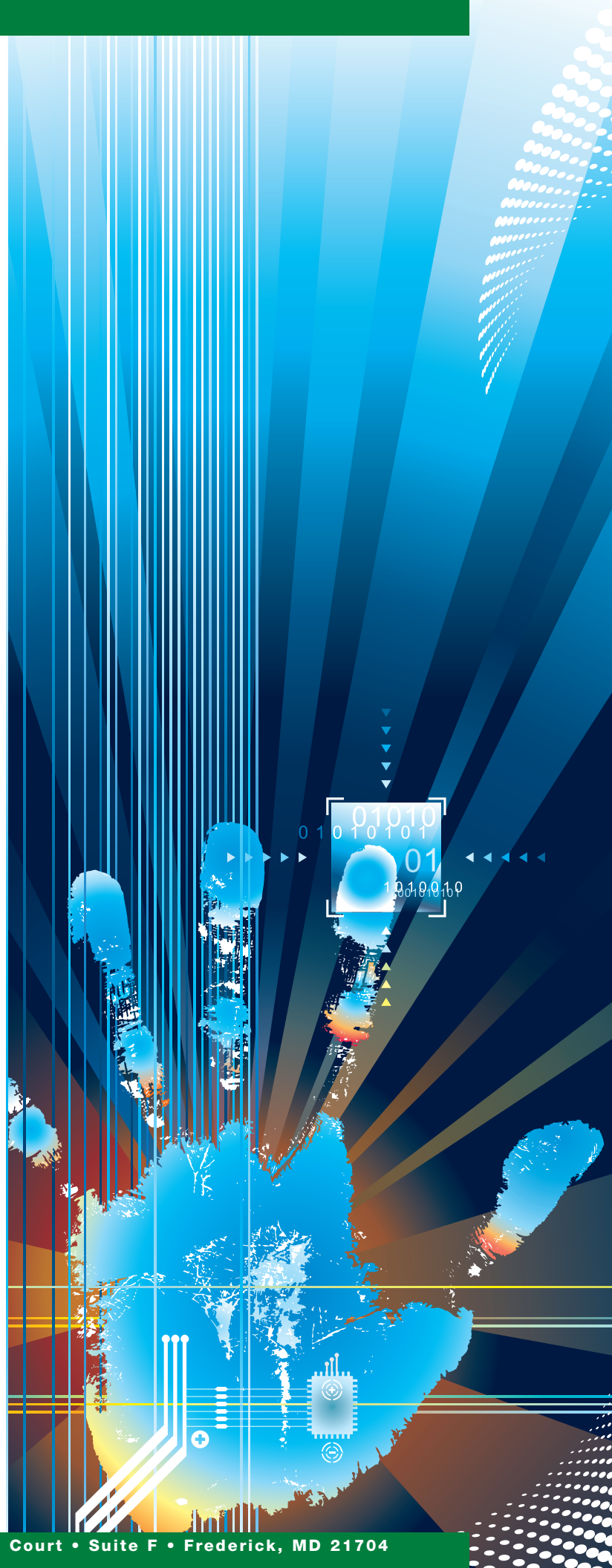
There have always been situations in which bodies external to a company impose requirements for tracking, controlling, and validating statements derived from information or the processes by which information is captured and managed within that company. Whether those requirements emanate from legislation, regulatory agencies, standards groups, or some other recognized authority—whenever there is some expectation of adherence of a company's IT infrastructure to a set of guidelines, we refer to that as compliance.

Through the Patriot Security Compliance service, we are able to assess your level of compliance, prescribe the steps necessary for compliance, and put in place the necessary protocols to ensure on-going compliance with the relevant guidance and regulations.

We're able to prescribe and assess the level of compliance that an organization exhibits with the following:

- **FISMA:** The Federal Information Security Management Act of 2002 is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002. The act recognized the importance of information security to the economic and national security interests of the United States, and requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Today's FISMA has brought attention within the federal government to cyber security and explicitly emphasized a "risk-based policy for cost-effective security".

When assessing an agency's level of FISMA conformity, Patriot's security consultants review every element of FISMA compliance, including but not limited to policies, procedures, configuration management, certification and accreditation/assessment and authorization, remediation plans, continuous monitoring, continuity of operations, and security awareness training. We then evaluate security and risk posture against the requirements and best practices established by the National Institute of Standards and Technology (NIST), identify gaps in the agency's security program and FISMA reporting, and provide detailed recommendations for remediating or maintaining compliance.



- **GLBA:** The The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act, includes provisions to protect consumers' personal financial information held by financial institutions. Passed by Congress due to growing concerns over identity theft and misuse of consumer financial information, the law requires financial institutions to adopt numerous measures concerning use, disclosure, and protection of the nonpublic personal information of customers. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule, and "Pretexting Provisions".

In assessing the level of GLBA compliance, Patriot's security consultants perform a detailed review of an organization's effort to manage and control risks to customer information. We review physical and logical access to customer information systems; customer information encryption policies and procedures, system change control, customer information system intrusion detection and prevention, attack response, and business continuity/disaster recovery. The result is an assessment of, and a roadmap for, the level of protection over customer information in line with the provisions of GLBA.

- **HIPAA:** The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that requires companies to adopt administrative, physical, and technical measures to protect the confidentiality, integrity, and availability of protected health information (PHI). Health care providers that conduct certain transactions in electronic form, health care clearinghouses, or health plans are deemed "covered entities" and are subject to HIPAA requirements.

In order to ensure compliance to HIPAA, Patriot performs a detailed assessment of Administrative, Physical, and Technical safeguards as detailed in the HIPAA Security Rule, determining what type of risks exist to the confidentiality, integrity, and availability of electronic PHI, evaluating the effectiveness of the safeguards, and recommending improvements to a covered entity's IT infrastructure and operation.

- **PCI DSS:** The Payment Card Industry Data Security Standards applies to all members, merchants, and service providers that store, process, or transmit cardholder data. Additionally, these security requirements apply to all "system components" which is defined as any network component, server, or application included in, or connected to, the cardholder data environment.

Patriot is able to perform a PCI DSS pre-audit (or "readiness") review to ensure that an organization is fully prepared for a full PCI Qualified Security Assessor (QSA) audit, with the intention of identifying un-met requirements that may result in loss of audit expenditure and ultimately audit failure. Our pre-assessments not only help build a baseline to ensure that compliance is achieved as efficiently as possible, but can also highlight findings that may be a liability for a company if not handled properly. Our pre-assessment will help you identify and learn about existing gaps between your current security posture and the PCI DSS, and will provide a head start in remediating identified gaps prior to the official PCI audit.

Patriot can help you cope with the shifting compliance landscape by interpreting a regulation or policy and how it affects your particular business, and then help you illustrate and prove to an external source that you have met the requirements of the regulation. By understanding the requirements themselves, justifying regulatory compliance, and then putting together the measures necessary to fully comply with the rules, Patriot can help you successfully build your compliance program, to the degree that makes sense to your business.

Patriot's deep experience in security software and hardware allows us to bring broad subject matter expertise across a number of vendor platforms. For example, we have current, extensive experience and certifications in the following solutions:



## Enterprise Lifecycle Security Specialists

Founded in 1996, Patriot Technologies is a privately owned, small business headquartered in Frederick, MD serving government and commercial organizations worldwide. To learn more about how Patriot's Professional Services can benefit your enterprise, call **301-695-7500** or visit **www.patriot-tech.com**.

GSA# GS-35F-4363D  
 We Accept IMPAC Visa Card  
 USDA BPA#AG-3142-B-08-0018  
 ESI SmartBUY# FA8771-07-A-0307 (Check Point)  
 NIH SmartBUY BPA# HHSN 263999900685B  
 BPA# W91QUZ-06-A-0005 (Websense)  
 SAIR SmartBUY BPA# GSQ0009AE0013 (BigFix)  
 Consulting and Technical Services (CATS) Contract  
 MD CATS Contract# 050R5800338

Other vehicles available: Encore II, Firstsource, ITES-2H, ITES-2S, NETCENTS, SEWP, Tiger, Treasury Commercial Vehicle (TCV), GSA Stars, Networkx, SDVOB and 8a partnerships, Arete Government Solutions, Leasing options

CAGE Code: 07FD4  
 DUNS: 933945248  
 Federal ID# 52-1957100



GSA Agent and Teaming Programs Available



Phone **301.695.7500**

Fax **301.695.4711**

02/12