



## Penetration Testing

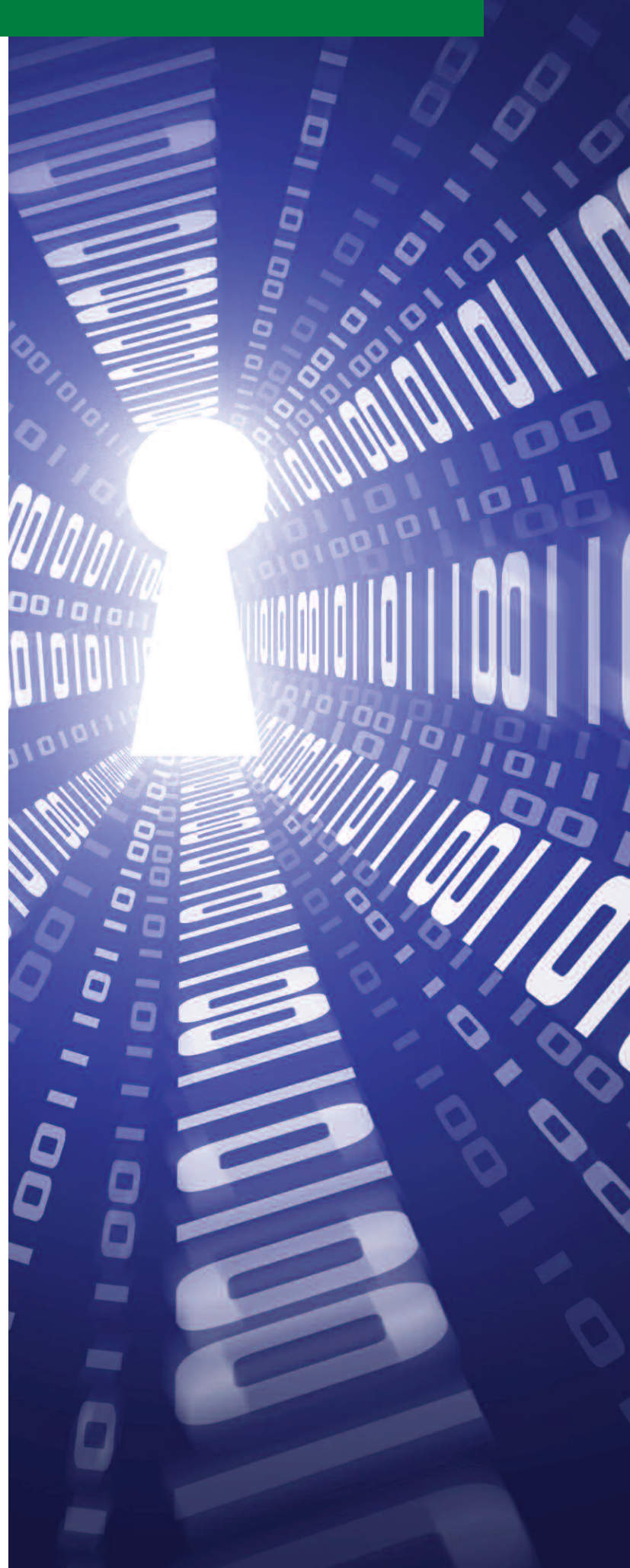
While many senior leaders may be aware that their systems and network house various vulnerabilities, a surprising few perform “proof-of-concept” testing by simulating an attack from a malicious source. Given today’s growth in sophisticated and advanced data breaches, an active analysis of system configurations, known and/or unknown hardware or software flaws, and/or operational weaknesses in process or technical countermeasures is clearly needed. Such testing needs to be carried out from the perspective of a potential attacker.

Through active penetration testing, Patriot’s security experts are able determine the feasibility of an attack and the extent of impact a successful exploit, if performed, may have. Our proven attack methodologies and vectors address the following:

- Network components (switches, routers, PBXs, VoIP)
- Desktop/laptop and mobile/wireless devices
- Database, DNS, and web servers
- IDS, IPS, firewalls, and proxies
- Web, email, cloud, and other internet-based applications
- Social engineering, client-side attacks, and brute force techniques
- Related aspects of physical security, e.g., data center access

Our penetration tests are more than just “ethical hacking”, as they are intended to:

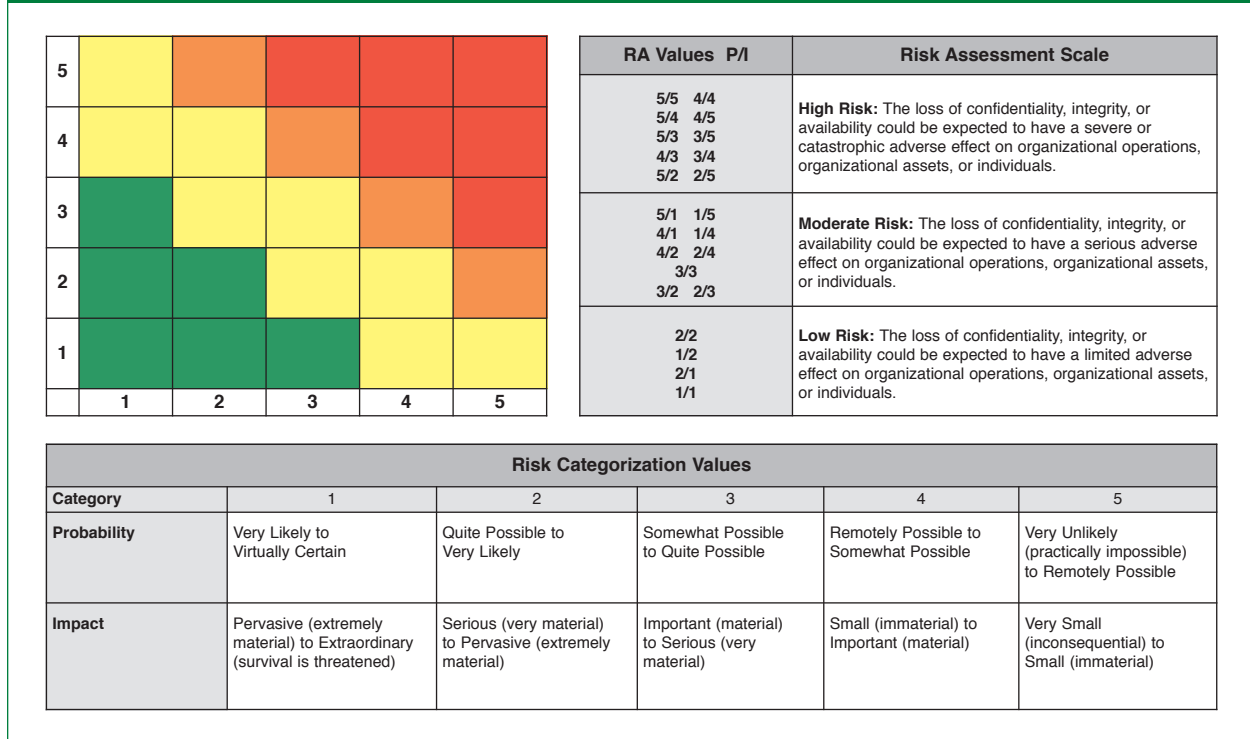
- Identify key information assets that require protection and the potential threats and likely adversaries
- Determine the effectiveness of existing and planned countermeasures for key assets
- Determine the degree of risk of each key asset
- Provide prioritized countermeasure recommendations
- Provide a roadmap of remedial actions as well as integrated and collective costs



The Patriot Penetration Testing is based upon generally accepted testing methods for detailed reconnaissance, deep scanning, exploitation, pivoting, and management reporting—tailored to maximize the value of testing from a management, technical, and risk perspective. We utilize the most current COTS and open source penetration testing tools and work closely with security operations personnel to ensure that any critical security issues found are resolved immediately. Additionally, we are able to provide a full risk-ranked assessment of likelihood and impact of an attack and recommended risk treatment (remediate, transfer, or accept).

The result is an extensive analysis that truly evaluates your security and prepares your defenses against the real thing—that is, finding vulnerabilities before an attacker does.

## Loss Impact and Probability



The Patriot "Risk Map" is used to assess the probability and impact of a particular risk occurring. When performing a penetration test, we plot each finding on this map in order to rank the likelihood and consequences of an exploit occurring, allowing for the most serious threats and vulnerabilities to be addressed.

## 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

**Schedule**  
 Contract GS-35F-4363D  
 GSA Agent and Teaming Programs Available



**Phone 301.695.7500**  
**Fax 301.695.4711**