



## Vulnerability Assessment

For many organizations, the exponential growth in systems, networks, and mobile devices in use across the enterprise creates a challenge in identifying, quantifying, ranking, and prioritizing vulnerabilities at an acceptable level and frequency demanded in today's environment. As a result, these organizations are at risk to inside or outside attacks, data breaches, and other IT failures.

In order to protect critical infrastructures as well as information, people, equipment, facilities, and operations, a comprehensive systematic evaluation of vulnerabilities and careful application of countermeasures is needed in order to improve overall security and reduce risk.

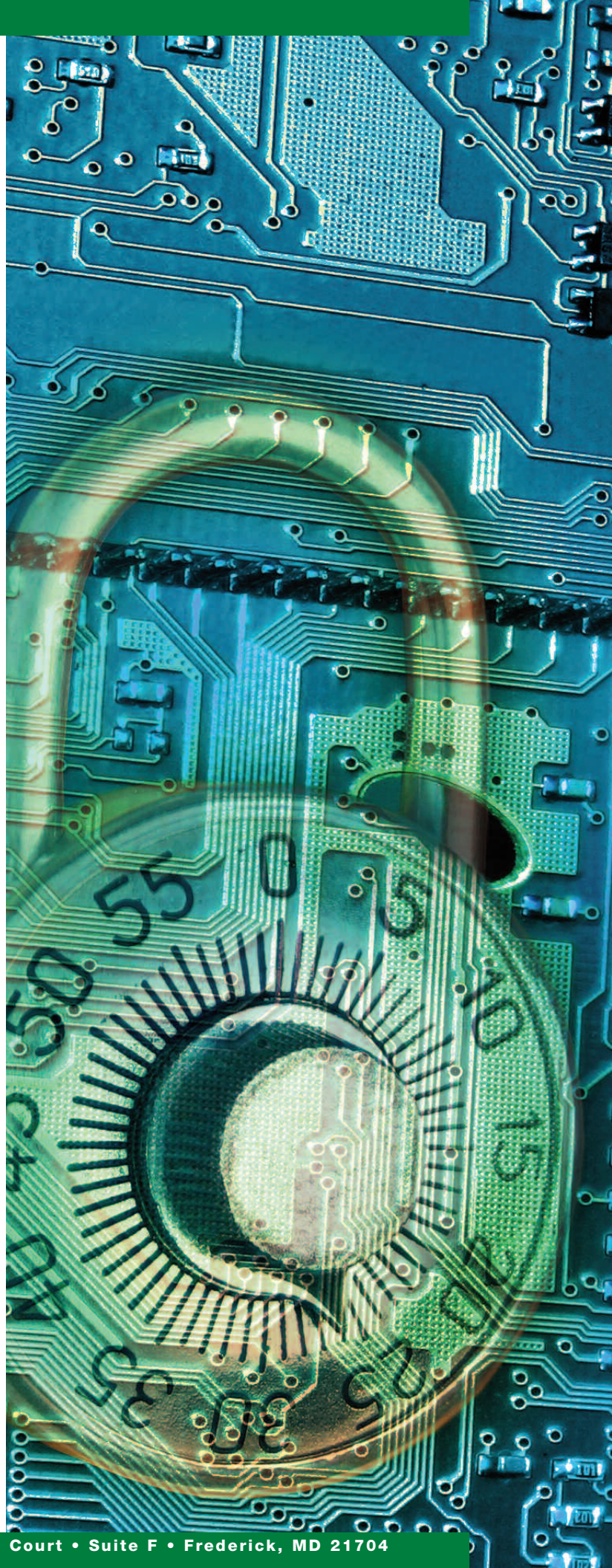
Patriot is able to perform an extensive assessment of these vulnerabilities by performing the following steps:

- Cataloging and classification of information resources (systems, networks, applications, devices, etc.)
- Assigning value and importance to these resources
- Identifying the vulnerabilities and potential threats to each resource
- Ranking the level of risk to these resources by the likelihood and impact of compromise

Patriot's comprehensive approach to a Vulnerability Assessment takes into consideration vulnerabilities across all information assets, including, but not limited to:

- Network assets, such as routers, switches, VPN concentrators, PBXs, VoIP devices, and wireless access points
- Computing assets, such as desktops, laptops, mobile devices, and servers
- Security assets, such as IDS/IPS, firewalls, anti-virus, and SEIM services
- Web assets, such as eCommerce, Web 2.0, DNS, web sites, and cloud services
- Application assets, such as databases, transaction processing services, and messaging

In addition, the Patriot Vulnerability Assessment can include a review of an organization's Situational Awareness and Incident Response (SAIR) capabilities, operational protocols, policies and procedures, and other compensating controls to determine the level of risk that exists.



Through the use of state-of-the-art network, application, and database scanning tools—combined with rigorous scheduling and project management protocols and a unique risk-based perspective—Patriot provides a timely and effective assessment methodology that can improve an organization’s risk posture on an on-going basis.

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:



## Loss Impact and Probability

5	Yellow	Orange	Red	Red	Red
4	Yellow	Yellow	Orange	Red	Red
3	Green	Yellow	Yellow	Orange	Red
2	Green	Green	Yellow	Yellow	Orange
1	Green	Green	Green	Yellow	Yellow
	1	2	3	4	5

RA Values P/I	Risk Assessment Scale
5/5 4/4 5/4 4/5 5/3 3/5 4/3 3/4 5/2 2/5	<b>High Risk:</b> The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
5/1 1/5 4/1 1/4 4/2 2/4 3/3 3/2 2/3	<b>Moderate Risk:</b> The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
2/2 1/2 2/1 1/1	<b>Low Risk:</b> The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Risk Categorization Values					
Category	1	2	3	4	5
<b>Probability</b>	Very Likely to Virtually Certain	Quite Possible to Very Likely	Somewhat Possible to Quite Possible	Remotely Possible to Somewhat Possible	Very Unlikely (practically impossible) to Remotely Possible
<b>Impact</b>	Pervasive (extremely material) to Extraordinary (survival is threatened)	Serious (very material) to Pervasive (extremely material)	Important (material) to Serious (very material)	Small (immaterial) to Important (material)	Very Small (inconsequential) to Small (immaterial)

The Patriot “Risk Map” is used to assess the probability and impact of a particular risk occurring. When performing a Vulnerability Assessment, we plot each finding on this map in order to rank the likelihood and consequences of a weakness being exploited by a given threat, allowing for the most serious vulnerabilities to be addressed.

## Enterprise Lifecycle Security Specialists

Regardless of whether you need a security vulnerability assessment for regulatory compliance or if you truly want to protect your organization from loss of valuable data and/or operational down-time, Patriot Technologies Vulnerability Assessment provides a thorough analysis and objectivity to accomplish your goals.

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

01/12