



# Raytheon Cybersecurity Solutions

## Protecting Critical Information from the Most Complex Threats



**Raytheon's defensive solutions protect against breach, fraud, theft and sabotage, while our offensive solutions target the identification and remediation of attack vectors used by today's most sophisticated cyber adversaries.**

Protecting America's critical networks and infrastructures is a constantly evolving challenge. Our open and technologically complex society presents a huge array of targets. Defending our systems, networks and infrastructures is vital to our economic and physical well-being.

Leveraging more than 30 years of building and protecting information systems, Raytheon offers leading-edge, integrated cybersecurity solutions that safeguard mission-critical systems against the widest range of internal and external threats. Raytheon's defensive solutions constantly monitor and protect against breach, fraud, theft and sabotage while our offensive solutions target the identification and remediation of attack vectors used by today's most sophisticated cyber adversaries. Raytheon provides robust, full-spectrum, advanced cybersecurity systems to protect our customers' critical

information networks and infrastructures from the most complex threats.

From Vulnerability Assessments to Information Assurance, Monitoring and Traffic Analysis to Information Operations, Raytheon is trusted by global governments and Fortune 500 companies to deliver a proven, powerful line of cyber defense.

### **Vulnerability Assessments**

How vulnerable is your organization? Are you prepared for possible disruption, espionage or sabotage to your critical systems?

Critical infrastructures, businesses and government facilities are vulnerable to various levels of violence and terrorism. Identifying and assessing these vulnerabilities help mitigate likely threats, securing intellectual property and protecting personnel.

Raytheon's vulnerability and security assessment solutions provide customized assessments

for government agencies, businesses, airports, seaports, water and power utilities, natural gas systems nuclear plants SCADA facilities and more. These insights help organizations safeguard against possible intrusions or attacks.

Our security assessments utilize an effective combination of integrated tools, techniques and trained and certified personnel.

### **Enterprise IA Solutions**

Government agencies are focused on protecting and improving the sharing of information, yet it is increasingly difficult to distribute data between varied security classification environments. Raytheon's cross-domain and multiple-domain information sharing solutions provide effective interoperability to ensure that data maintains its designated sensitivity level throughout the information sharing and transmission processes.

Raytheon's leading information-sharing solutions bridge the security gap between and inside domains, resulting in a high-speed, efficient and cost-effective information-sharing solution, even for the most challenging data environments.

### **Monitoring and Traffic Analysis**

Cybersecurity threats are not always external. Increasingly, governments and businesses face risks to their critical networks and systems from their own employees, whether the incident is malicious or accidental.

Insider risk management involves a continuous process of risk assessment, policy definition for mitigating those risks, situation analysis and remediation of problems that occur. Raytheon's award-winning insider threat protection solutions proactively defend against internal threats, constantly monitoring and protecting against breach, fraud,

data and intellectual property leaks, theft and sabotage. We leverage our years of experience with the highest levels of endpoint monitoring and focused observation across America's most critical classified networks.

## Information Services

An ongoing security issue is the exploitation of vulnerabilities in software operating systems and applications. Many attacks against systems, by both hackers and malicious software, now begin with a foothold being established

through a known vulnerability in the target system and the software it is running. The scale of these attacks has significantly increased in recent years.

Raytheon provides world-class vulnerability and open-source exploitation technologies, stopping hackers in their tracks.

## Information Operations

Raytheon offers best of breed reverse engineering services to support offensive and defensive information warfare capabilities. Our massively scaled software

platforms enable discovery of security vulnerabilities and malicious code, whether embedded, on servers or workstations.

We possess world-class automated malware detection and discovery, quick turnaround spyware and malware analysis, forensic binary analysis, development of covert software agents and implant tool chain components, exploit development, emulation, disassembly and debugging, as well as vulnerability analysis of existing hardware and software systems.

No matter how complex the system or threat, Raytheon's integrated cybersecurity solutions protect the confidentiality, integrity and availability of critical information and infrastructures – with total assurance.

## Robust Portfolio of Cybersecurity Products and Technologies

- **Vulnerability and Security Assessments**
  - Physical and Information Security Assessments
  - Software Vulnerability Testing
  - Penetration Testing
  - Certification and Accreditation
  - Compliance and Security Audits
- **Enterprise Information Assurance (IA) Solutions and Services**
  - Cross-Domain and Multiple-Domain Information Sharing
  - Perimeter Defense
  - Public Key Infrastructure (PKI)
  - Security Architectural Engineering and Systems Integration
  - IA Training
- **Monitoring and Traffic Analysis**
  - Secure Voice/Video/Data Communications
  - Endpoint and Network Monitoring
  - Insider Threat Protection
  - Real-time Network Traffic Analysis
- **Information Services**
  - Cryptographic Solutions
  - Vulnerability Exploitation
  - Computer Network Defense (CND)/Computer Network Operations (CNO)
  - Open Source Exploitation
- **Information Operations (IO)**
  - Dynamic Defense
  - Reverse Engineering
  - IO Tools and Exploits
  - Tradecraft



*Raytheon ensures that critical information is not lost, corrupted or interrupted.*

For further information contact:

**Intelligence and Information Systems**  
P.O. Box 660023  
Dallas, TX 75266-0023 USA  
571.226.4832 phone  
iismedia@raytheon.com

**www.raytheon.com**  
Keyword: Cyber