



Information Assurance

At Mantis Security, Information Assurance is far more than IT and network security. For our DoD, IC, and Federal customers, critical infrastructure assets, mission data, and human lives depend on the protection of sensitive information. Our adaptive risk management practices help your security management team, from executives to engineers, effectively respond to the risks and security challenges of your rapidly evolving mission.

Our **IA Engineers** provide the expertise to better secure your systems, networks, and data, providing vital information to the people who need it—at the right time.

Our comprehensive services help you meet the security needs demanded by your information types, mission, and environment. Our compliance experts ensure that your risk tolerance aligns with ICD 503, CNSSI 1253, DODI 8510.01, and NIST SP 800-53 and 800-37. We create efficiencies in Vulnerability Management, the Risk Management Framework (RMF), and other executive orders or agency policies to reduce risks of system downtime, data compromise and loss.

Our IA team is experienced with implementing the RMF on a multitude of system profiles--from public/private cloud environments, to highly secure controlled access programs, to enterprise systems with high availability.

Our IA experts are CISSP and CISA certified and meet DoD 8570 requirements. We help protect your classified and protected information from network intrusion and understand that in many cases the front line of defense is right inside your own boundary where trusted users pose an inside threat.

Complete Information Assurance Services

- ❖ Security controls assessment (A&A, C&A) support
- ❖ IA engineering and security architecture design
- ❖ Security support, monitoring and training
- ❖ IA Policy transition and guidance
- ❖ IA Vulnerability Management (IAVM) support
- ❖ Threat and vulnerability risk assessments
- ❖ Information risk management

CONSULTING

From hackers and terrorists to equipment failure and natural disasters, numerous threats can compromise the confidentiality, integrity and availability of your data, putting your mission at risk.

ID	TITLE	Confidentiality			Integrity			Availability			
		L	M	H	L	M	H	L	M	H	
SC-27	Platform-Independent Applications										
SC-28	Protection of Information at Rest	+	X	X	+	X	X				
SC-28(1)	Protection of Information at Rest Cryptographic Protection	+	+	+	+	+	+				
SC-28(2)	Protection of Information At Rest Off-Line Storage										
SC-29	Heterogeneity										
SC-29(1)	Heterogeneity Virtualization Techniques										
SC-30	Concealment and Misdirection										

We understand risks and the importance of protecting against them and planning. We have a proven history of designing and building secure systems that are relied upon for classified and unclassified information for the national intelligence effort. We have leveraged this depth of experience to develop a full range of **Information Assurance Services** that go beyond typical IA offerings.

INFORMATION ASSURANCE

Technical Services

- ❖ Threat and vulnerability assessments
- ❖ Quantitative and qualitative risk assessments
- ❖ Risk remediation strategies
- ❖ IT strategy aligned to security
- ❖ IC ITE and FEDRAMP transition

IA Engineering and Architecture Design

- ❖ Security architecture evaluation and enhancement
- ❖ Application and web security
- ❖ Configuration Management planning
- ❖ Cloud and network security architectures
- ❖ Access control modeling (ABAC/DAC/MAC)

Certification & Accreditation (C&A)

- ❖ ICD 503 transition services
- ❖ DIACAP RMF services
- ❖ Implementation guide
- ❖ Plan of action and milestones (POA&M)
- ❖ ISSO management
- ❖ IA compliance consulting
- ❖ Automated continuous monitoring

Security Support and Training

- ❖ Security incident response
- ❖ Support for annual training and disaster recovery exercises
- ❖ Security program review and consultation
- ❖ Customized security mission continuity planning
- ❖ SDLC security process review