



## Integrated Cyber Solutions

### Overview

URS Corporation is a fully integrated engineering, construction and technical services organization with the capabilities to support every stage of the project life cycle—from inception through start-up and operation to decommissioning and closure. We offer program management; planning, design and engineering; systems engineering and technical assistance; construction and construction management; operations and maintenance; and decommissioning and closure services.

Combining forces with URS, Apptis now offers an expanded range of services. With deep experience in federal government driving the latest innovative technology advancements such as Cloud Computing, URS-Apptis is a fully integrated engineering and technical services organization delivering IT and communication services to federal agencies and all branches of the military.

### Core Capabilities

- Secure Cloud Computing
- Integrated Cyber Solutions
- Software Engineering
- Systems Engineering
- Enterprise Management
- Network Engineering
- Program Management

Our certified and accomplished professionals deliver information technology and infrastructure results.

Agencies face a growing challenge to provide an increasing level of data access to dispersed employee populations and citizens while mitigating an ever-expanding variety of cyber threats.

To secure sharing and collaboration with the public, as well as within and across agencies, URS-Apptis cyber experts apply proven solutions and trusted technology processes that monitor and verify the confidentiality, integrity, and availability of government information systems and communications. We partner with our customers to develop complete security architectures. Our solutions address the convergence of physical and cyber security and are integrated into existing Information Assurance programs, people, policies, and technologies to guarantee success. We ensure security is built in, not added on. URS-Apptis Integrated Cyber Solutions have been successfully used to secure technology investments and meet federal compliance standards.

- Preventative, ethical hacking against Department of Homeland Security Web applications to simulate malicious attacks.
- Developing the most secure identity/citizenship management system in the world—the U.S. Passport and Passport Card.
- Moving the Transportation Security Administration FISMA score from an F to an A in just 18 months, making it the first agency within Department of Homeland Security to achieve 100% Authority to Operate.
- Providing 24x7x365 IDS/IPS analysis of network traffic entering the Pentagon.

### Integrated Cyber Solutions Capabilities

- Business Continuity Planning & Disaster Recovery
- Certification & Accreditation, FISMA, NIST 800 Series, DIACAP
- Encryption Solutions/PKI
- Identity, Access, & Authentication Management & Credentialing
- IDS/IPS Management & Monitoring
- Information Risk Management
- Penetration Testing
- Security Engineering, Architecture, Auditing, Assessments
- Security Operations Center Development & Management
- Security Policy Development
- Vulnerability Management, Patch Remediation

### Certifications

- Certification & Accreditation Professional (CAP)
- Certified Business Continuity Professional (CBCP)
- Certified Ethical Hacker (CEH)
- Certified Information Security Manager (CISM) Certified Information Systems Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- National Security Agency INFOSEC Assessment Methodology Certification (NSA-IAM)

### Representative Clients

- Coast Guard
- Defense Acquisition University
- Defense Information Systems Agency
- Defense Threat Reduction Agency
- Department of Defense—Pentagon
- Department of State
- Federal Emergency Management Agency
- Transportation Security Administration

4800 Westfields Boulevard  
Chantilly, VA 20151  
Phone: 703-745-6016  
E-mail: [info@apptis.com](mailto:info@apptis.com)

[www.urscorp.com](http://www.urscorp.com)

## Proof of Performance



Network Security Services for the Pentagon

### U.S. Army Information Technology Agency, Network Infrastructure Services and Operations – Pentagon (NISO-P)

URS-Apttis provides network security services to the NISO-P Directorate of Security, including information systems engineering and integration, for the Office of the Secretary of Defense, Army, and Air Force components of the Pentagon information technology enterprise. The network security tasks involve detecting threats and denying access to organizations or individuals that wish to steal, intercept, or modify the classified and “sensitive” but “unclassified” information that is contained within the Pentagon information technology enterprise. URS-Apttis also performs periodic assessment of the structure and configurations of the Pentagon networks and sub-networks to identify vulnerabilities. The scope of this effort extends around the world.



Cyber Security

### Military Healthcare System Cyberinfrastructure Services

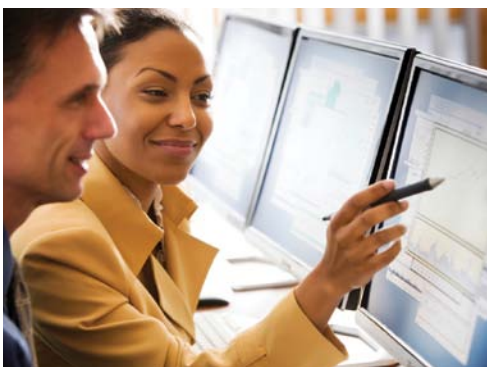
We provide on-site network engineering and administration for the Military Healthcare System Cyberinfrastructure Services, ensuring efficient daily information management in support of the U.S. Armed Forces. This work includes security at DoD hospitals, clinics and remote sites in the United States, Europe and Asia.



Network Engineering

### Defense Information Services Agency (DISA) Command Center, Cyber Command (CYBERCOM)

URS-Apttis stands 24/7 Information Assurance watch in the newly formed DISA Command Center providing cyber security engineers to DISA on the DISN Global Services contract performing Computer Network Defense Service Provider Tier II support including Incident Response Analysis, IA Compliance and supporting the planning and analysis of future Computer Network Defense solutions to help defend the backbone of the DoD Global Information Grid.



IT Support

This same project supports USCYBERCOM to ensure the situational awareness on the globally deployed Defense Information Systems Network (DISN), the backbone of the DoD Global Information Grid (GIG), is provided in real time to the Director of Current Operations of USCYBERCOM. URS-Apttis personnel assist the JOC Battle Captain to shape the DISN and bring to bear all of DISA’s assets in support of Commander, USCYBERCOM’s guidance and intent to shape the DoD cyberspace battlefield in support of defense cyber objectives, and immediate response to cyber threats and incidents.

URS-Apttis implements recommended changes to policies, procedures, and technologies to foster continuous enhancement of theater IA/CND posture and capabilities. Our Team supports the prioritization of IA/CND tasking for the DSE Network Assurance Branch Chief, theater Information Assurance Manager (IAM) and NETOPS Center (SWO).

### IT Support Service Task Order for United States Forces-Iraq J6 Communications Directorate (USF-I J6)

URS-Apttis has supported the U.S. Army in active combat zones with skilled and qualified engineers with deep knowledge and theater-mission experience. At present, we support seven locations for the United States Division - Center, providing management engineering services, integration of enterprise infrastructure, and telecommunications support. URS-Apttis incorporates Capability Maturity Model Integration (CMMI) Level 3, ISO 9001:2008, Program Management Institute (PMI), Help Desk Institute (HDI), Information Technology Infrastructure Library (ITIL), and other industry standard practice guidelines to meet the unique needs of the USF-I J6. Our professional technical staff includes systems engineers, network engineers, information assurance engineers, integration engineers, software engineers, and support technicians with certifications including: CISSP, CISCO CCIE, CCNA, CCNP, Microsoft MCSA, MCSE, SharePoint, ASP.Net, Visual Studio, VB.NET, and SQL, among others.