

## Cybersecurity Services & Commodities

Ready to meet your agency's cybersecurity mission? NITAAC, a Best in Class (BIC) Government-Wide Acquisition Contract (GWAC) program office, offers a wide array of cybersecurity products and services through its contracts to help your agency enhance security, improve and protect mission critical information and more!

Our three BIC vehicles boast streamlined acquisition for fast ordering through a single-login electronic-Government Ordering System (e-GOS). With built-in guidance, automated task order completion and ceiling rates negotiated at the Master Contract Level, NITAAC has got your agency covered when it comes to cybersecurity!

### NITAAC Cybersecurity Benefits



Designated BIC by the Office of Management and Budget (OMB) and the Government-Wide Category Management Program Management Office.



Quickly obtain a variety of cybersecurity solutions.



GWAC orders use streamlined processes and procedures under FAR 16.505 vs. the rigorous source selection process under FAR Part 15.



Cybersecurity products and services are available from industry leading Contract Holders under CIO-SP3, CIO-SP3 Small Business and CIO-CS.



## Overview

**CIO-SP3** and **CIO-SP3 Small Business** can accommodate cybersecurity services under Task Area 7: Critical Infrastructure Protection and Information Assurance. The objective of Task Area 7 is to support the protection of critical infrastructure, assurance of agency information and operations that protect and defend information and information systems by ensuring confidentiality, integrity, availability, accountability, restoration, authentication, non-repudiation, protection, detection, monitoring and event react capabilities. A comprehensive, but not limited, sampling of work to be performed under this task area, includes:

Task Area 7		
Cybersecurity	Disaster Recovery	Cryptographic Support & Services
Records Management	Public Key Infrastructure	Security Certification & Accreditation
Training and Awareness Programs	Facility Protection Planning	Information Systems Security
Exercises and Simulation	IT Forensics and eDiscovery	Application Security
Identity Management & Assurance	Risk Management (Vulnerability Assessment & Threat Identification)	Trusted Internet Connections Implementation
Information Assurance of Critical Infrastructure	Critical Infrastructure Continuity and Contingency Planning	Incident Response Planning and Execution
Security Review and Analysis of Automated Information Systems	Intelligent, Automated Data Collection and Analysis	Security Operations Center Development & Operations Management
Critical Infrastructure Asset Identification and Configuration Management Databases	Federal Information Security Management Act (FISMA) Implementation Support	Health Insurance Portability & Accountability Act Implementation Support

**CIO-CS** can accommodate Cybersecurity under Category 3: IT Security Software.

**Category 3A:** All Anti-Virus, IT Security, Authentication, Authorization, Identification, Firewall, Management and Monitoring Software, Encryption, Forensic Analysis, Security and Management Tools.

**Category 3B:** Renewals, Subscriptions, Support and Licenses to any Software that falls under group 3A.

A comprehensive, but not limited, sample of IT Security Software Commodities, includes:

Commodities	
Anti-Virus Software	Biometric Identification Software
Authentication and Authorization Software (includes Single Sign on and Two Factor Authentication)	Public Key Infrastructure (includes Digital Certificates)
Forensic Analysis Tools	Encryption Tools
HIPAA Assessment Software	Patient Identification Software
Network and Host Based Intrusion Detection & Prevention Software	Vulnerability Scanning, Assessment and Management Software
Remote Device Management Software	Security Information Event Management Tools
Log Management Tools	Enterprise Network Firewalls
Data Loss Prevention Software	Security Analytics
Vulnerability Assessment Software	Continuous Monitoring Software