NETCENTRICS
SECURE OUR NATION

Capabilities Overview



A Mission-Centric Approach

Since 1995, NetCentrics has consistently advanced its mission to secure our nation by thriving in the evolving digital and threat landscape.

Over the past three decades, we've firmly established ourselves as leaders in cybersecurity, cloud and digital transformation, while supporting defense, homeland security, federal civilian, and intelligence sectors.

Our dedication to those safeguarding our freedoms inspires us to innovate and stay ahead of adversaries. Our commitment to excellence ensures we remain vigilant and proactive.



(703) 714-7345

205 Van Buren St. Suite 420
Herndon, VA 20170

www.netcentrics.com

bd@netcentrics.com

About NetCentrics

Your Mission, Our Priority

For 30 years, NetCentrics has excelled as an innovative technology solutions provider for the U.S. government, evolving into a trusted partner dedicated to guarding national security through relentless innovation.

We are proud of our growth and expertise in cybersecurity, cloud and data AI as we consistently deliver cutting-edge solutions and critical mission support to ensure secure, uninterrupted operations.

In a digital battleground filled with dangerous adversaries, we stay at the forefront of innovation, meeting and exceeding the evolving security needs of our customers.

Excellence is our duty, and we are honored to serve, protect, and innovate for the United States federal government.

Partner with us in securing the nation's digital domains and fostering a safer future.



Our Focus Areas

Cyber Security

The cyber threat landscape is constantly evolving, and so is NetCentrics. We are dedicated to delivering modern and customized solutions to our customers, ensuring they are mission-ready. Our support extends to TTP development for the U.S. Coast Guard and National Guard, as well as providing services and capabilities such as SOC, CSSP, CSOC, NOSC, and Cyber Protection teams. With our advanced engineering expertise, we offer the right solutions and expert personnel to outsmart adversaries in any cyber situation. Partnering with NetCentrics means securing your network, mission, people, and desired outcomes.

Cloud Security

The cloud serves as the battleground for the "invisible war in cyberspace" and embodies the evolving nature of today's cyber threats. Trying to safeguard our civilian and national defense cloud assets by relying on outdated defensive tools is ineffective and irresponsible. At NetCentrics, we recognize the need to stay ahead of adversaries who are fast, sophisticated and constantly developing new ways to take advantage of cloud vulnerabilities. By leveraging a community approach and partnering with leading technology providers, we bring the best cloud security solutions to your mission. Our offerings include Wraith, a cloud-native, multi-terrain visibility and threat hunting Security-as-a-Service platform.

Our Focus Areas

Digital Transformation

NetCentrics is your trusted partner in digital transformation, to include our dual-use commercial and government AI Platform. Additionally, we have a long history of expertise in everything from implementing Zero Trust Architecture and cloud to legacy IT. We understand the resources, expertise and investment needed for network and IT infrastructure modernization. Our team excels in AP, automation, cloud migration, architecture development and application management, providing successful outcomes for projects of any size. With a focus on operational excellence, we prioritize identity verification, access controls, and continuous monitoring to ensure the utmost security and resilience for your digital assets.

Mission Support

NetCentrics supports and furthers the DoD agencies' mission with expertise in strategic consulting, program management, research, analysis and training. We provide a comprehensive services portoflio spanning tactics development, strategic communications, information security systems management (ISSM), test support and software development. We identify, prioritize, and remediate threats and vulnerabilities, design risk mitigation strategies, and assist with strategic planning to support our national defense customers' mission-critical objectives. We also possess expertise in systems engineer technical assistance (SETA) and advisory & assistance services
(A&AS).

Our Organizational Capabilities

NetCentrics boasts a team of elite engineers and security specialists, including both contracted professionals and in-house experts, leading the way in embracing the latest and emerging technologies for our esteemed customers. We've expanded our capabilities to include targeted innovations and strategic investments, specifically designed to meet the urgent challenges of cybersecurity and cloud security in today's digital landscape. Our commitment is to deliver mission-critical support through unparalleled solutions, addressing the most pressing challenges and threats. Our cyber and cloud expertise includes but is not limited to:



Cyber Security

- Wraith multi-cloud C2 and threat hunting solution
- Zero Trust Design / Implementation
- CSSP Management and Support
- Assessment and Authorization (A&A)
- Classified Network Modernization
- Application Rationalization
- PKI/ICAM Design/ Implementation
- Cyber Protection Teams
- Risk Management
- ISSO
- Security Assessor
- Digital Forensics



Cloud Security

- Multi-Cloud and Hybrid Cloud Security
- IaC
- Cloud Networking
- Cloud Security Posture
- Information Assurance
- Service Integration
- SaaS Expertise
- CI/CD-DevSecOps-QA/Testing
- Containerized Compute
- Cloud Migration
- Edge Computing



Digital Transformation

- Arbor AI Platofrm
- Large Scale IPv6 Migration
- Infrastructure Support/ Engineering
- Enterprise Architecture
- Advanced Analytics
- SharePoint Administration
- Virtualization
- PKI Management
- Tier I & 2 Help Desk Support
- AV/VTC Architecture
- VIP Support



Mission Support

- Strategic Ris Remediation
- SETA
- A&AS
- Strategic Cyber Advisory Services
- Government Stakeholder Expertise
- Regulatory Research Policy Development
- Cyber Gaps & Opportunities Assessments
- Project Program Management
- Quality Assurance
- Technical Writing
- Training

THE AI SYSTEM OF WORK PLATFORM

Arbor

One reasoning layer for the entire mission.

Arbor turns the systems and data you already have into governed facts, runs your agents over them as one system, and returns an explainable recommendation a person approves.

Dual-use by design — proven in commercial production, running on government missions today.

From NetCentrics — a national security company that builds software. 31 years.



DUAL-USE

Running in commercial production at Fortune 500 scale and on government missions today. Industry-proven technology, not a development program.

YOURS

You are buying an ontology you get to keep. Replace us and the semantic model stays with the government.

WEEKS

Weeks to a working decision, not years to a platform. A pilot lands at $100–250K and proves it.

1.2B
records reconciled in production

50,000+
explainable decisions a day

99.9%
uptime across five regulated industries

Arbor is mature before you buy it — the platform does not change; only the mission ontology is built for you. Not FedRAMP High or IL5/IL6 accredited today; an ATO is pursued per deployment.

Core Capabilities

WHAT MAKES ARBOR DIFFERENT

Government-Owned Ontology

You are buying an ontology you get to keep. Replace us and the semantic model and mission logic stay with the government. No data-rights encumbrances on your data or anything derived from it — clean under MOSA and DFARS.

Orchestrated, Not Siloed

Most agencies are accumulating disconnected AI pilots. Arbor runs agents as one system on one shared ontology — passing work between them, over the same governed facts, under one policy and one audit trail. Any model, any agent.

Grounded Reasoning

The knowledge graph holds resolved facts; only the agents infer. Every conclusion traces back to the exact facts that produced it, with provenance and a calibrated confidence a watch officer or a JAG can read.

Securing the Agent

We build the agents and we defend them. When an agent can act, the question becomes who constrains it — tool misuse, privilege escalation, exfiltration through reasoning. Thirty years of cleared cyber operations behind the answer.

Built for Six Mission Functions

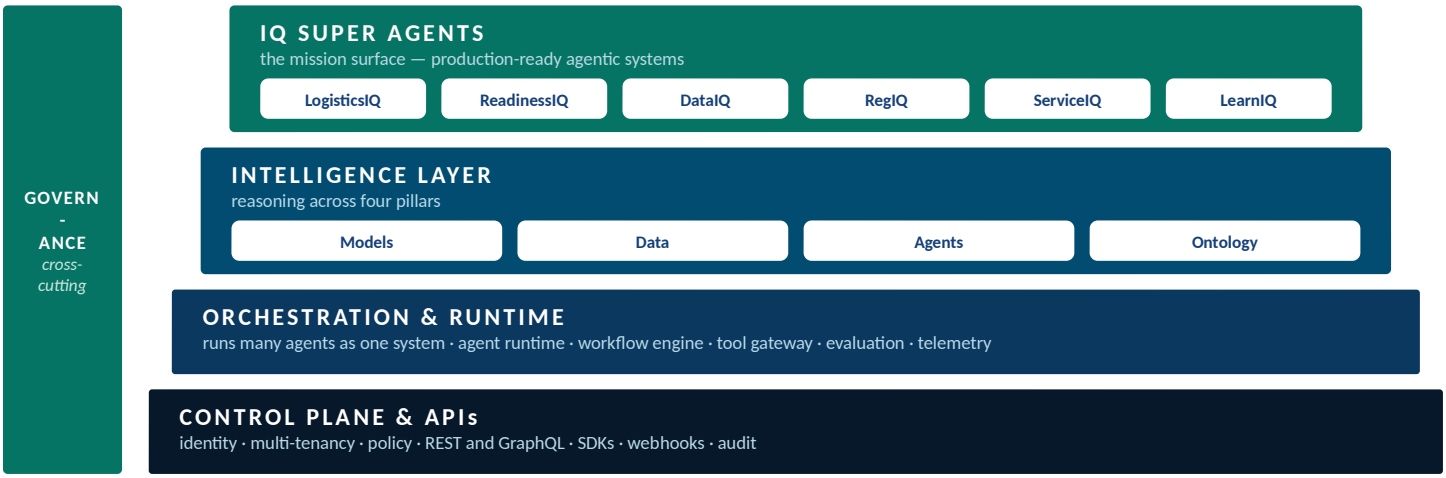
ONE ONTOLOGY, RE-POINTED — EACH EXPANSION CHEAPER THAN THE LAST



The platform is function-agnostic. The mission ontology is what gets built on top — so the second use case inside a function never starts from zero.

Platform Architecture

A LAYERED INTELLIGENCE STACK



Governance spans every layer — trust and safety, auditability, security, compliance, observability. Arbor is engineered against IL5/IL6 control requirements; an Authorization to Operate is pursued per deployment.

How Arbor Works on a Problem

ONE STRICT SEPARATION OF CONCERNS — WHICH IS WHAT MAKES IT EXPLAINABLE

01 RESOLVE

Records scattered across systems collapse into one entity, every source kept beneath it.

Six part records, four systems, one radar amplifier.

02 ASSESS

An agent weighs the situation against that entity's own history, not a generic baseline.

Three airframes depend on it. Ninety days of stock.

03 RECOMMEND

An explainable recommendation with the authority it rests on and a calibrated confidence.

Reclaim rather than buy new. Evidence attached.

04 DECIDE

The call and its full audit trail pass to the person who owns the decision.

Supply request raised. A human signs.

Many sources in, one approved decision out. The knowledge graph holds the facts and only the agents infer — which is what lets any conclusion be traced back to the facts that produced it.

Agents We Have Already Built

EACH ONE A MISSION ONTOLOGY ON THE SAME PROVEN PLATFORM

These are not shelf products. The platform, the agent framework and entity resolution at scale do not change — what gets engineered for you is the ontology for your mission. Which is why the second agent inside a function costs less than the first — and why they run as one system, not six.

LogisticsIQ *Readiness and supply chain*
Models supplier, materiel and regulatory constraints to catch disruption early.

DataIQ *Data and financial integrity*
Finds anomalies, improper payments and reconciliation breaks, and explains why.

RegIQ *Preventive compliance*
Embeds FMR, OMB A-123 and agency policy into workflows, enforced before action.

ServiceIQ *Case and service intelligence*
Turns service-desk, benefits and FOIA casework into consistent, governed decisions.

LearnIQ *Workforce development*
Skill graphs and sandboxes so cleared personnel and agents develop together.

HealthIQ *Health mission*
Clinical, operational and regulatory data with safety and compliance guardrails.

Why NetCentrics

A NATIONAL SECURITY COMPANY THAT BUILDS SOFTWARE · 31 YEARS

Thirty-One Years in National Security
Delivering inside defense, intelligence and federal civilian networks since 1995. Cleared, and accountable for what we field.

Problem Solvers by Trade
We take data, process and decision problems — the quality of a call and the time it takes to make it.

Sovereign by Design
Built for on-premise, disconnected and classified environments — and we deploy inside your boundary.

Land and Expand
One ontology powers every new agent — each expansion cheaper than the last.

NETCENTRICS

Three ways to buy AI for mission work

For government decision-makers. The choice is between three architectures, not three vendors.

	ARBOR NetCentrics	THE DATA PLATFORM Lakehouse and data infrastructure	THE FULL-STACK PLATFORM Integrated mission platform, one vendor end to end
What it is	An AI System of Work. A reasoning layer — ontology, knowledge graph and agents — sitting on top of your existing systems of record and disparate data sources.	A lakehouse. Infrastructure to land, store, govern, and compute over data. You supply the mission logic, the engineers, and the years of development.	A full-stack platform with real agentic capability: it reasons over fused data and recommends action. Integration, ontology, applications and workflow from one vendor — all or none.
Ontology ownership	You do — an ontology you get to keep. Replace us and the semantic model stays with the government.	No mission ontology exists. You own the catalog and schema you build yourself, starting from zero.	The ontology lives inside the platform. Leaving means leaving the modeled meaning behind.
Data rights & exit	You own your data and everything derived from it. Clean under MOSA and DFARS. Exit cost is low by design — that is the point.	Your data is yours; the platform is not. Pipelines, jobs, and models are rewritten if you move.	Ask what you can take with you on the first day after non-renewal. Deep adoption across the services raises switching cost — by design.
Cost posture	Sized to the problem in front of you. A pilot lands at $100–250K and proves the use case — an order of magnitude less to start.	Consumption-based. Compute and storage costs grow quietly and permanently.	An exquisite platform at an exquisite price. Minimum engagement near $1M plus a resident engineering team, against ceilings in the hundreds of millions.
Fit to mission	Purpose-built around your mission, your requirements, and your data. The solution conforms to the organization.	Neutral substrate. It conforms to nothing until you build on it.	Configured to you by the vendor's own engineers, on a model built for the enterprise. The organization adapts more than the platform does.
Where it works	Any function with fragmented data and a decision at the end — logistics, readiness, operations, finance, IT and cyber, workforce.	Anywhere in principle. In practice, wherever you can fund the engineering to build the mission logic yourself.	Broad in principle. In practice it lands where an enterprise agreement can be justified, which concentrates it in operations and intelligence.
Architectural lineage	Built in the current AI era. Agentic reasoning, multi-modal Q&A and forecasting grounded in the ontology — traceable and defensible.	A real advance over the data warehouse, but a storage-and-compute paradigm, not a reasoning one.	Ontology and platform lineage predate the agentic era. The agentic capability is real, and it was layered onto a foundation designed for analysis.
Time to value	Weeks to a working decision, not years to a platform. A new requirement is absorbed by the ontology, and we are small enough to make it the priority.	Months to stand up, then the mission logic is still ahead of you. Value arrives when your engineers finish building on it.	Enterprise adoption on the platform's timeline. A new requirement is scheduled against a roadmap shared with every other customer.
Securing the agent	We build the agents and we defend them. When agents can act, the question becomes who constrains them — backed by thirty years of cleared cyber operations.	Governance for data and models. No answer for an agent that can act on systems of record.	Strong platform security. The agent-assurance question — tool misuse, privilege escalation, exfiltration via reasoning — remains unanswered.

THE BOTTOM LINE The full-stack platform can probably do it. The questions are what it costs, how long you wait behind every other customer, and who owns the meaning afterwards. The data platform sells you the materials. Arbor delivers the reasoning layer over the data you already have and leaves the ontology in government hands — with the people who know your mission.

We Are Cloud & Security Experts



Infrastructure As Code (IaC)

- Defining a range of cloud objects as code (ARM, Bicep, Terraform)
- Deploying cloud objects leveraging cloud infrastructure
- Defining object configurations as code before deployment
- Managing secrets/licensing for deployed objects
- Managing namespaces for copied objects
- Deploying cloud environments meeting the DoD Secure Cloud Computing Architecture (SCCA) framework, such as Azure Mission Landing Zones (MLZ)



Cloud Networking

- Defining large-scale networks in IaC
- Pre-determined security zones and risk mitigation
- Extensive network separation via subnetting and micro-segmentation
- Defining security appliance settings/ rules as IaC before deployment
- Experienced with network/app gateways providing secure access to services
- SD-WAN/SASE/CASB and VPN incorporation



Cloud Security Posture

- Expertise in compliance requirements and best practices
- Defining security mitigations into each object
- Implementing/managing cloud-based impact levels in multiple environments
- Managing environment access vectors and least privilege
- Managing RBAC/Zero Trust environments
- Security assessments and testing



Multi-Cloud

- Extensive cloud service provider (Azure, AWS, GCP, OCI) experience
- Cloud-to-cloud interoperability
- Multi-cloud metrics and security telemetry management
- Insights into CSP strengths and weaknesses
- Multi-cloud redundancy / high availability

Information Assurance



- Data normalization across varying sources
- Dynamic data structures for utility
- Data pipelines for mass ingestion
- Data enrichment for at scale
- Data housing with high performance solutions
- Data visualization to answer questions of the dataset
- Expert data engineering

Service Integration



- Expertise in combining disparate services on demand to fill customer requests
- SASE Integration
- SaaS Integration
- Cloud to cloud + On-prem to cloud
- Conducting analysis of alternatives for technology solutions
- Solutions architecting
- Identity integration

SaaS Expertise



- Implementing SaaS solutions when appropriate
- Securely integrating into existing security architecture
- Managing identities and data
- Codify SaaS configurations as IaS

CI/CD - Devsecops - QA/Testing



- Defining cloud resources as objects to be managed with automated pipelines (ADO, Gitlab Pipelines, Team City, Jenkins)
- Experienced with operationally testing resources
- Automated testing & vulnerability analysis
- Building and maintaining changelogs and SBOMS for complex environments
- Dynamic/static tests for quality
- Managing secrets for automated workflows
- Time-based or event-based pipeline triggering



Containerized Compute

- Transitioning legacy servers/virtual machines to scalable containerized technology
- Building/managing/deploying Kubernetes clusters
- Container networking and name spacing
- Managing dynamically mounted persistent storage for containerized compute
- Securing containerized architectures
- Managing code images at scale
- Vulnerability/change management/SBOMS in containerized environments



Cloud Migration

- Significant CSP (Azure, AWS, GCP, OCI) experience
- Experienced with workflows to manage migration of critical resources
- Managing data loss risk
- Updating manually defined objects as IaC
- Cost-benefit analysis/business analysis
- Cost management
- Security impact analysis
- Optimizing for scale and redundancy



Edge Computing

- Experienced with existing edge computing solutions
- Implementing edge computing solutions when appropriate
- Expertise in security concerns of edge computing devices
- Azure stack edge
- Understanding use cases and managing challenges

US Coast Guard: 14 Years of Partnership



Since 2011, NetCentrics has diligently worked to foster a close partnership with the U.S. Coast Guard, successfully performing numerous cybersecurity, digital transformation and IT projects in support of multiple USCG missions. This included large projects with the Telecommunications & Information Systems Command (TISCOM), Command, Control, Communication, Computer, Cyber and Intelligence Service Center's (C5ISC) Shared Services Division 1 in Alexandria, VA, and USCG Cyber.

Most notably, NetCentrics has served as a 24x7 Cybersecurity Service Provider (CSSP) for USCG for over a decade, safeguarding its critical digital assets and infrastructure against sophisticated adversaries. Our commitment to continued training and skills development of our cybersecurity team contributed to the evolution and implementation of modern cybersecurity frameworks within USCG's Cyber Operations. By harnessing the power of real-time monitoring tools, scrutinizing system logs, and leveraging advanced threat intelligence capabilities, NetCentrics proactively identified emerging threats, investigated potential security breaches, and implemented effective countermeasures to mitigate risks.

Further expanding collaboration with the USCG, NetCentrics lent technical and operational expertise to successfully stand up the Coast Guard's Cyber Protection Teams (CPTs). Our technicians automated the installation of software and data configurations on the CPT kits using Infrastructure as Code (IaC), reducing the time between notification and execution of a response mission from five business days to under 24 hours. We also integrated the ability to monitor and secure operational technology (OT) into the kit as part of the Coast Guard's mission to secure critical infrastructure against cyberattacks.



NetCentrics' cyber expertise accelerated the Coast Guard CPTs' ability to conduct operations. We developed an advanced emulation capability, tactics, techniques, and procedures (TTPs), a training program, and provided tech support, among a host of other support capabilities. NetCentrics personnel even deployed with the CPTs for both exercises and real-world operations.



US Coast Guard: Key Projects

U.S. Coast Guard (USCG) Network Operations & Security Center (NOSC)

Over the span of 13 years, NetCentrics has supported USCG's mission as a 24x7 Cybersecurity Service Provider (CSSP), contributing to the evolution and implementation of modern cybersecurity frameworks within USCG's Cyber Operations. Keenly focused on maintaining a round-the-clock hub for monitoring, detecting, analyzing and responding to security incidents and threats, NetCentrics has played a pivotal role in fortifying USCG's cybersecurity posture. All roles in support of the USCG program required cleared personnel with TS/SCI and CI polygraph.

NetCentrics employed a comprehensive array of methodologies encompassing real-time monitoring, integration of threat intelligence and rapid incident response protocols. These measures were designed to bolster the resilience, integrity and protection of the USCG's digital assets across both the Non-Classified Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) segments of the Department of Defense Information Network (DODIN). By harnessing the power of real-time monitoring tools, scrutinizing system logs and leveraging advanced threat intelligence capabilities, NetCentrics proactively identified emerging threats, investigated potential security breaches, and implemented effective countermeasures to mitigate risks.

NetCentrics emphasizes the importance of continuous training and skills development to ensure that cybersecurity professionals stay abreast of the latest trends, technologies and methodologies in the field. By investing in the ongoing education and professional development of its team members, NetCentrics strengthens its capacity to address evolving cyber threats and challenges effectively. This commitment to training and skills enhancement not only boosted the capabilities of individual cybersecurity professionals but also reinforced NetCentrics' ability to deliver unparalleled support to the USCG in safeguarding its critical digital assets and infrastructure against sophisticated adversaries.

Cyber Protection Teams / Incident Response Teams

Operating under the ethos of being a "quick strike team," as articulated by Cleophus Thomas, the former director of operations (J3) at JFHQ-DODIN, Cyber Protection Teams (CPTs) are specialized teams adept at swiftly identifying, containing and mitigating cyber incidents before they escalate. As the Coast Guard stood up Cyber Protection Teams, NetCentrics' scope expanded to include not only the NOSC, but also support of their CPTs.

NetCentrics' technical and operational expertise was central the Coast Guard's success. NetCentrics technicians automated the installation of "clean" software and data configurations on the CPT kits using Infrastructure as Code (IaC), reducing the time between notification and execution of a response mission from five business days to under 24 hours. We also integrated the ability to monitor and secure operational technology (OT) into the kit as part of the Coast Guard's mission to secure critical infrastructure against cyberattacks.

Moreover, NetCentrics' cyber operations experience accelerated the Coast Guard CPTs' ability to conduct operations. We developed an advanced emulation capability, tactics, techniques, and procedures (TTPs), a training program, and provided tech support, among a host of other support capabilities. NetCentrics personnel even deployed with the CPTs for both exercises and real-world operations. The totality of NetCentrics' support resulted in laudatory CPARs ratings from the Coast Guard:



"Given what I know today about NetCentrics' ability to perform in accordance with this contract or order's most significant requirements, I would recommend them for similar requirements in the future."

KEITH MINER
Contracting Officer, US Coast Guard

US Coast Guard: Feedback & Accolades

"The NetCentrics team is multifaceted and able to flex throughout the organization to ensure mission success, planning and execution."

"On top of your projects and JQR [Job Qualification Requirements] efforts, your expertise is a valuable day-to-day resource for questions from all analysts, qualified and unqualified, as well as questions from team leads."

"We utilized the process that was developed in no small part with the NetCentrics' team's assistance, and it worked perfectly. This help saved us a lot of time and frustration."

"The NetCentrics team's Master Analysts are all capable of handling highly complex missions and demonstrating daily that their knowledge and experience is highly valued by the Coast Guard Cyber Programs."

"The kudos provided by the USCG CPT Mission Element Lead expressed gratitude for the knowledge and expertise that the NetCentrics staff provided. This was the first time the team started the mission in less than 30 minutes onsite due to the staff's technical knowledge and presence."

US Coast Guard: NetCentrics' Contract Overview



$39M

SUPPORT SERVICES (LABOR) – NETWORK OPERATION SECURITY CENTER (NOSC)

PSC CATEGORY	NAICS CATEGORY
IT AND TELECOM – NETWORK SUPPORT SERVICES (LABOR)	CUSTOM COMPUTER PROGRAMMING SERVICES

2017-2024

USCG CONTRACTING OFFICE
C5I DIVISION 1 ALEXANDRIA

$100M

USCG C4IT SC IT/IA SECURITY MANAGEMENT SERVICES Indefinite Delivery Contract

PSC CATEGORY	NAICS CATEGORY
IT AND TELECOM – OTHER IT AND TELECOMMUNICATIONS; OTHER ADP & TELECOMMUNICATIONS	OTHER COMPUTER RELATED SERVICES

2011-2017

USCG CONTRACTING OFFICE
TISCOM

$41M

OTHER TECHNICAL ENTERPRISE SUPPORT SERVICES (TESS) BPA Contract

PSC CATEGORY	NAICS CATEGORY
IT AND TELECOM – INTEGRATED HARDWARE/SOFTWARE /SERVICES SOLUTIONS, PREDOMINANTLY SERVICES	CUSTOM COMPUTER PROGRAMMING SERVICES

2015-2020

USCG CONTRACTING OFFICE
TISCOM

DISA:
A 28-Year Partnership

Since 1996

NetCentrics has forged a successful partnership with Defense Information Systems Agency (DISA) and performed numerous IT infrastructure and services projects in support of multiple Pentagon agencies under the DISA umbrella, including the Washington Headquarters Services (WHS) and Joint Service Provider (JSP).

In 2016

NetCentrics was awarded the Compute and Application Services (CAS) contract to provide IT services in support of JSP's mission of managing and defending the Department of Defense's key cyber terrain, particularly in the Pentagon and National Capital Region. This $50M+ firm fixed price contract included one base year and two option years. NetCentrics and its partners assisted the JSP in its mission to be a customer-focused organization that provides, manages, operates and maintains IT shared services for the Pentagon and select agencies and organizations in the capital region.

2019-2023

NetCentrics' relationship with DISA included a four-year, $268.5M contract to provide information technology support to the WHS to assist in their mission for managing the Department of Defense enterprise infrastructure. NetCentrics performed this work 2019-2023 at various locations within the National Capital Region, including the Pentagon and Mark Center.



NetCentrics became one of the awardees for the Encore III multiple-award IDIQ contract vehicle spanning 2018-2028 term enabling us to provide a full range of IT services and solutions required by the Department of Defense and other federal agencies, including DISA.

The current NetCentrics JSP AV/VTC Support Services contract involves providing audio-visual and video conference support services. The NetCentrics team is responsible for managing inventory levels, maintaining accountable records, and overseeing the maintenance of JSP AV/VTC endpoint hardware and software components. Recently, the NetCentrics AV/VTC team, in collaboration with our partner CompQsoft, supported the Presidential Transition Office (PTO) by ensuring all its needs and requirements were met. The team's extraordinary commitment, working days, nights, and weekends, enabled the PTO to perform its mission effectively. The NetCentrics staff was fully dedicated to providing the highest level of service to the team that will guide our nation through the next four years, resulting in a resoundingly successful Inauguration Day.

DISA: Feedback & Accolades

"NetCentrics' exceptional project management skills and ability to collaborate effectively with cross-functional teams have been key factors in driving the successful completion of this undertaking."

"NetCentrics' unwavering commitment, tireless dedication, and remarkable expertise have been instrumental in working towards achieving this crucial milestone for our shared customer."

"The NetCentrics team's comprehensive understanding of the complex regulatory landscape, coupled with their meticulous attention to detail, has enabled them to navigate the intricate processes involved with remarkable finesse."

NetCentrics continues to deliver the best-in-class service. This enables the team to succeed and achieve results at a rapid pace that would not be possible without their support."

Beyond their technical expertise, the NetCentrics unwavering dedication to our team's mission and their passion for upholding the highest standards of quality and security have been truly inspiring."

"As the leadership wanted to ensure the first 2-3-star level forum is a success, the NetCentrics team showed up in the afternoon just to be on standby as we brought up the system, which worked with no flaws."

"Great job in regards to your attention and support to the Joint History Conference last week. Keep up the good work!!"

DISA: NetCentrics' Contracts Overview

Contract	Duration	SIZE	NAICS Category	PSC Category
JSP Computer And Application Services (CAS)	2016-2018	$50M	541511: Customer Computer Programming Services	7020: Information Technology Central Processing Unit (CPU), Computer, Analog) D316: IT and Telecom - Telecommunications Network Management D399: IT and Telecom - Other IT and Telecommunications
Washington Headquarters Services (WHS) IT Support	2019-2023	$268.5M	541513: Computer Facilities Management Services 541511: Customer Computer Programming Services	D799: IT and Telecom - Other IT and Telecommunications R499: Support-Professional: Other 7030: ADP Software
Base Operations and Support Services (BOSS) contract	2019-2024	$75M	541511: Customer Computer Programming Services	D399: IT and Telecom - Other IT and Telecommunication
JSP Back Office Support Services	2017-2025	$18K	541512: Computer Systems Design Services	R425: Support-Professional: Engineering/Technical
OA-22 HQ Computer and Application Services	2016-2025	$25.5M	541511: Customer Computer Programming Services	D302: IT and Telecom - Systems Development
Audio-Visual and Video Conference Services For The JSP	2024-2025	$10.8M	541519: Other Computer Related Services	D316: IT and Telecom - Telecommunications Network Management

Federal Trade Commission: A 20-Year Partnership

Since 2004, NetCentrics has been cultivating a strong relationship with the Federal Trade Commission, culminating in a blanket purchase agreement (BPA) award for IT support services as a prime vendor. Under this BPA, NetCentrics has received multiple task orders, including End User Support Services (EUSS) contract currently valued at $104M, delivering FTC Enterprise Service Desk (ESD) support across all FTC locations and organizations to enhance the FTC mission.

In 2019, the FTC awarded NetCentrics a $35.5 million contract for the FTC Information Technology Support Service (ITSS) Blank Purchase Agreement (BPA) which lasted until 2024.

The NetCentrics staff have worked closely with FTC employees performing IT support services and received numerous accolades for their problem-solving abilities, prompt, courteous service and exceeding customer expectations.

Feedback & Accolades

"I'd like to commend NetCentrics employee X and his colleague for their outstanding customer service this morning. They went above and beyond to assist me with a faulty monitor, demonstrating exceptional professionalism and courtesy. Please convey my sincere gratitude to them."

William T. Merkle, Deputy CIO, FTC

"NetCentrics has helped with so many things lately, I don't even know that I can keep track. They are truly an asset."

"I really appreciate how quickly you all were able to resolve my issue! Thanks so much!"

"Excellent assistance, very prompt, and cordial to staff – thank you!"

FTC: NetCentrics' Contracts Overview

Information Technology Support Services (ITSS) Blank Purchase Agreement (BPA)

2018-2024

Size: **$35.5M**

NAICS CATEGORY

541511: Custom Computer Programming Services

PSC CATEGORY

DA01: IT & TELECOM- BUSINESS APPLICATION DEVELOPMENT SUPPORT SERVICES (LABOR)

D399: IT & TELECOM- OTHER IT & TELECOMMUNICATIONS

Regional Offices Wiring Project

2006-2007

Size: **$195K**

PSC CATEGORY

R499: SUPPORT - PROFESSIONAL: OTHER

NAICS CATEGORY

238210: Electrical Contractors & Other Wiring Installation Contractors

End User Support Services

2019-2024

Size: **$104M**

NAICS CATEGORY

541519: Other Computer Related Services

PSC CATEGORY

DA01: IT& TELECOM BUSINESS APPLICATION/ APPLICATION DEVELOPMENT SUPORT SERVICES (LABOR)

D399: IT & TELECOM- OTHER IT & TELECOMMUNICATIONS

Business Admin Services, IT Hardware, IT Software, IT Consulting, Program Management, IT Outsourcing

2004-2024

Size: **$148M**

PSC CATEGORY

DA01: IT & TELECOM - BUSINESS APPLICATION/ APPLICATION DEVELOPMENT SUPPORT SERVICES (LABOR)

D399: IT & TELECOM- OTHER IT & TELECOMMUNICATIONS

NAICS CATEGORY

541511: Custom Computer Programming Services

541512: Computer Systems Design Services

Wraith: Cross-Cloud Visibility & Threat Hunting

Wraith, NetCentrics' cutting-edge cloud visibility solution, stands at the forefront of addressing the evolving challenges in cloud environments. With its robust patent-pending capabilities, Wraith provides comprehensive insight into the complex landscape of cloud infrastructure, allowing organizations to monitor and analyze their resources effectively. Most organizations monitor the state of each of their clouds in silos. Wraith centralizes signals from all cloud providers into one dataset, so security professionals can easily monitor user activity and track cloud state changes. Wraith captures cloud telemetry through an engineered set of data connectors and data ingest pipeline. The solution plays a critical role in enhancing cybersecurity measures by quickly identifying potential vulnerabilities and ensuring compliance with industry regulations.

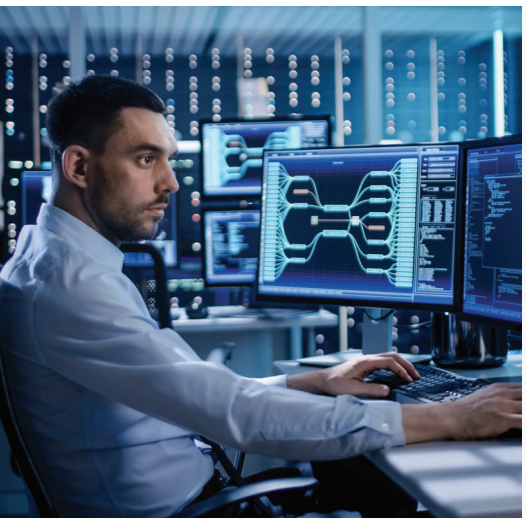
Wraith empowers organizations with real-time visibility, aiding in strategic decision-making and resource allocation. As organizations navigate the evolving cloud threat landscape, Wraith emerges as a crucial ally, offering visibility and control to maximize the efficiency and security of cloud operations. The largest barrier to security in cloud environments is simply understanding the ecosystem. Wraith enables immediate situational awareness of cloud objects from all cloud vendors in one place, with one query language. Wraith is packaged with workbooks to enable teams to quickly understand their environments and allows easy access to the wider detection community and all the associated tools.



We Are Cloud & Security Experts

Omni-Cloud/Cross-Cloud Visibility

By integrating tools like Wraith, NetCentrics is not only contributing to the resilience and agility of federal operations but also playing a crucial role in shaping a future where the United States can confidently navigate the complexities of the digital age, safeguard its interests, and assert its leadership on the global stage. These solutions enhance visibility, foster a refined security posture, and offer a simplified approach to monitoring environments for operators as they mitigate potential vulnerabilities within the multi-cloud infrastructure.



As multi-cloud configurations become increasingly mainstream, the government sector is feeling the need to shore up these vulnerabilities in the name of securing the nation, and so are actively seeking avenues to simplify complexity and address the twin challenges of security and redundancy. Innovative solutions like Wraith are stepping into this space for federal and state agencies, offering a harmonizing layer that simplifies the intricacies of omnicloud management. While the path may be fraught with potential market resistance and the demands of self-implementation, the overarching goal remains steadfast: to achieve streamlined omnicloud management with ease-of-use in mind.

In an evolving digital landscape, it is imperative for enterprises to adapt and refine their approach to managing omnicloud environments. The focus is increasingly on enhancing visibility and fortifying security within these complex structures, ensuring that the full potential of cloud investments is harnessed. In this transformative era, the nuanced role of sophisticated solutions like Wraith is gaining prominence. These solutions are not merely tools but strategic partners, empowering enterprises to navigate the complexities of omnicloud environments with confidence and providing the strategic insights necessary for success.

It's time to take a decisive step towards mastering your omnicloud environment. Ask yourself: do you have complete visibility into your cloud infrastructure? Can you confidently track every change and addition across your multi-cloud terrain? If the answer is anything but a resounding yes, then it's time to acknowledge a critical gap in your cloud strategy and take action.

We Are Your Strategic Cyber Advisory Partner

Government Stakeholder Expertise

NetCentrics has worked hard to cultivate a reputation of excellence throughout a wide range of government organizations. As a leading strategic cyber advisor, we know the right people to coordinate with and the best ways to engage them.

Key Stakeholders Include:

- The Office of the Secretary of Defense
- Department of Defense Joint Staff
- Federally Funded Research & Development Centers (FFRDCs)
- The Defense Information Systems Agency (DISA)
- The Intelligence Community (IC)





Regulatory Research & Policy Development

We pride ourselves on our ability to quickly identify and manage a wide breadth of regulatory requirements. These requirements serve as a solid strategic backbone for executive decision-making and cyber modernization and policy planning.

Our strategic advisors are well versed in executive requirements from IC directives (ICDs) to Joint Pubs to National Security Presidential Memorandums (NSPMs) and more. We specialize in applying this knowledge in the form of policy development recommendations and insights.

We Are Your Strategic Cyber Advisory Partner

Cyber Gaps & Opportunities Assessments

Federal agencies have a finite number of resources at their disposal and may have blind spots when it comes to cyber strategy and policy, as well as technology modernization efforts.

Our strategic advisors assess cybersecurity risks and vulnerabilities for critical sectors and develop phased action plans to close cyber gaps and optimize new opportunities.

Strategic Risk & Remediation Strategies

Federal agencies are not immune to ever-increasing risks and threats. NetCentrics offers an objective expert voice to help senior members of the DoD and national security agencies identify, prioritize and remediate threats and vulnerabilities, design risk mitigation strategies, and assist with strategic planning to realize their vision and mission-critical goals.

Remediation plans can include manpower, budgetary, software/hardware and policy/directive recommendations to safeguard organizations and teams of any size.

Our strategic advisors assess cybersecurity risks and vulnerabilities for critical sectors and develop phased action plans to close cyber gaps and optimize new opportunities.

Our strategic advisors also have a successful track record of working with supply chain partners to understand and mitigate 2nd and 3rd-party risks, foreign investment risks, and more.



INDOPACOM Modernization: Many IT enterprises suffer from a conglomeration of decisions across different functional entities that ultimately results in a suboptimal architecture requiring many personnel to maintain and has fragmented data repositories and applications. NetCentrics provided detailed recommendations to create better resiliency, leverage data, and to secure data no matter where it resides.

Technology Partnerships

We maintain vital partnerships with industry-leading technology providers which allow us to bring best-in-class technologies to bespoke solutions for the government.
These partnerships grant us access to the latest offerings before they are publicly available, provide reach-back access to the builders, develop internal subject matter expertise and influence future features – while driving down costs for our customers.
Our partner relationship with Microsoft has influenced the way it approaches multi-cloud threat visibility and resulted in uplift of Azure capabilities to GovCloud.

Technology Partners

Trellix
VECTRA
EQUINIX
FORTINET
vmware
tenable
aws
DELL
CompTIA
Microsoft
eclypsium
SWIMLANE
aruba
a Hewlett Packard Enterprise company
paloalto NETWORKS
Gigamon
RACKTOP
SUPERMICRO
Google Cloud Platform
ORACLE CLOUD
Microsoft Azure

Open Source Solution Partners

Wiki.js
rocket.chat
SURICATA
zeek
GitHub

ANC/NHO Partners

Copper River
ECHELON SERVICES

Contract Vehicles

GSA MAS

NetCentrics is a prime contract holder on the General Services Administration Multiple Award Schedule (GSA MAS) contract vehicle. GSA MAS is a flexible, long-term Indefinite Delivery, Indefinite Quantity (IDIQ) contract that provides government buyers with access to millions of commercial products and services at pre-negotiated prices.

- SIN 54151HACS – Highly Adaptive Cybersecurity Services (HACS)
- SIN 54151S – Information Technology Professional Services
- SIN 541990 – All Other Professional, Scientific, and Technical Services (Non-IT)
- SIN 541990TAD – Technical and Engineering Services (Non-IT)
- SIN 611430 – Professional and Management Development Training
- SIN OLM – Order-Level Materials
- SIN 541990AV – Professional Audio/Video Services

OASIS+ Unrestricted

NetCentrics is a prime contract holder on the One Acquisition Solution for Integrated Services (OASIS)+ Multi-Agency Contract (MAC). Oasis+ is a government-wide, multiple-award, Indefinite Delivery, Indefinite Quantity (IDIQ) acquisition program for complex professional services and innovative solutions from highly qualified firms on a contract vehicle designed to be the next generation Best-in-Class (BIC) contract.

Missile Defense Agency SHIELD IDIQ Award

NetCentrics was awarded a position on the Missile Defense Agency's Scalable Homeland Innovative Enterprise Layered Defense (SHIELD) Indefinite-Delivery/Indefinite-Quantity (IDIQ) contract with a $151B ceiling. This strategic vehicle enables the rapid delivery of innovative, mission-critical capabilities in support of the warfighter through flexible and agile task order execution. This award reflects the strength of NetCentrics' technical expertise, operational excellence, and business development capabilities, as well as the continued trust and confidence placed in our team by our government partners.

SeaPort Next Generation (SeaPort NxG)

NetCentrics is a prime contract holder on SeaPort NxG, the Navy's electronic platform for acquiring support services in 23 functional areas including Engineering, Financial Management and Program Management.

SEWP VI (Solutions for Enterprise-Wide Procurement)

NASA's SEWP VI is a Government-Wide Acquisition Contract (GWAC) designed to streamline the procurement of IT products and services for federal agencies. We provide a breadth of advanced technology and cybersecurity solutions to the government through this contract vehicle.

Contract Vehicles

DLA and ONIX Rapid Acquisition Methods

DLA Tailored Logistics Support (TLS) — Estimated 2–3 Weeks

DLA Tailored Logistics Support (TLS) enables rapid procurement of mission-critical equipment, software, and related services through pre-competed prime vendor contracts. TLS provides a streamlined acquisition path for Arbor deployments tied to logistics modernization, operational technology, and integrated mission support. Award timelines can be as short as 2–3 weeks

ONIX
Open
National
Innovation
Exchange

ONIX OTA (Open National Innovation Exchange) — Estimated 4–6 Weeks

ONIX is a flexible OTA vehicle administered by Army Contracting Command–Rock Island for rapid acquisition of innovative commercial technologies, prototypes, and production capabilities. Well suited for AI, automation, and logistics modernization, ONIX enables Arbor pilots and scaled deployments with significantly reduced contracting friction. Award timelines can be as short as 4–6 weeks



Key Customers

Performance Track Record

This performance overview highlights key contract aspects, such as size, scope, complexity, relevance, clearance level, use of cloud-based solutions, and support for various tiers and cybersecurity measures across the projects.

The consistent presence of these elements indicates a robust track record in meeting diverse requirements.

Requirements	JSP Boss	OSD EITSD	WRAITH Cloud Security Solution	USCG NOSC	USCG C4IT IA
Size	$75M	$450M	$5.45M	$39M	$100M
Scope	YES	YES	YES	YES	YES
Degree of Complexity	High	High	High	High	High
Recent & Relevant	YES	YES	YES	YES	YES
Clearance level	TS/SCI	TS/SCI	TS/SCI	TS/SCI & CI-Poly	TS/SCI & CI-Poly
Cloud - Based Solutions	YES	YES	YES	NO	YES
Tier 1-3 Support	YES	YES	YES	NO	YES
Cybersecurity	YES	YES	YES	YES	YES



NETCENTRICS

SECURE OUR NATION

October 2026