

Government Programs

Ingalls Is the Department of Defense Cybersecurity Solutions Expert

Ingalls is the next generation of Cybersecurity Service Providers (CSSPs). We offer a full suite of technology-enabled, integrated cybersecurity risk management services. Our team is leading development and implementation for the Cybersecurity Assurance Readiness (CSAR) Process and the Cybersecurity Maturity Model Certification (CMMC).

With diverse experience across military/defense intelligence, network security, information technology and cybersecurity solutions, our expertise focuses on four business lines of service:

- Managed Detection and Response
- Incident Response
- Professional Services
- Government Programs

Core Capabilities

- Incident Response Remediation & Ransomware Negotiations
- Information System Security Manager (ISSM)
- Information System Security Officer (ISSO)
- DoD Authorization to Operate (ATO) Support
- Cybersecurity Assurance Readiness (CSAR)
- CMMC Registered Practitioner Organization (RPO)
- Virtual CMMC Registered Practitioner (vCMMC RP)
- DIBCAC Preparation
- DoD Risk Assessments
- Gov Managed Detection & Response (GovMDR) - Coming Soon
- Viewpoint, Patented Cybersecurity Data Visualization

Cybersecurity Maturity Model Certification (CMMC) Registered Practitioner Organization (RPO)

Let us help you navigate CMMC and DFARS. As a key player in the cybersecurity industry, we know what it takes to secure and protect our nation's IT infrastructure. We provide comprehensive solutions to support CMMC practices and are ready to help DoD contractors prepare for a CMMC assessment.

Ingalls is part of the CMMC ecosystem and is a trusted advisor bound by a professional code of conduct from the Cyber Accreditation Body (AB) formerly CMMC AB. We stand ready to provide advice, consulting, and recommendations to clients. Our cyber knowledge will support your journey to becoming CMMC ready.

Ingalls performs a CMMC Pre-Assessment Readiness Review with the client with the following tasks:

- Prepare for CMMC
- Conduct Interviews and Review Evidence
- Generate Gap Analysis Report and Plan of Action & Milestones
- Perform Vulnerability Assessments



CSAR, Your Best Hope for ATO Survival.

The Department of Defense (DoD) has a mission to field systems at the "speed of innovation" while ensuring cybersecurity requirements are met. Existing Authorization to Operate (ATO) processes are exhaustive, resource-intensive, and often not considered until the application is ready to deploy, significantly delaying timely delivery of today's technology to the warfighter.

DoD must shift from a cybersecurity snapshot in time and paper drill compliance culture to a culture where automation and real-time continuous risk monitoring is tightly coupled with supply chain risk management and integrated software development pipelines (DevSecOps). The Cybersecurity Assurance Readiness (CSAR) tool advances this culture shift.

CSAR empowers Users to make smart, timely decisions allowing applications to be adaptive and keep pace with cybersecurity threats and vulnerabilities.

Authorization To Operate (ATO) Support

The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is a 7-step process that organizations can use to manage information security and privacy risk



FutureFeed is the step-by-step tool for completing your NIST SP 800-171 and CMMC cybersecurity compliance requirements. The intuitive user interface and carefully designed questions streamline the hardest parts of any compliance program: data collection and decision making. FutureFeed is designed from the ground up to help you get compliance right the first time, and prove it anytime.

CSAR Software Offers:

- ✓ Efficiency through an intuitive TurboTax-like interface for the ATO process, transforming mandatory forms into easy, manageable sections
- ✓ Automatic mapping of data input minimizing memory load and eliminating question redundancy
- ✓ RMF timeline and risk profile feedback based on user input, adjusting ATO path for a more secure option
- ✓ The ability to easily address required RMF Action Path processes, building threat matrices, and informing risk while the application is being developed, baking security in from the outset, not bolting it on as an afterthought
- ✓ A dashboard view for visibility of key cybersecurity controls assessed in the software pipeline combined with operational and management controls for supply chain risk management
- ✓ Cyber Playbooks and Plans for a secure cyber roadmap
- ✓ A technology enabled solution with expert "Human-in-the-Loop" support at key Checkpoints enabling your application to be Cyber Ready

for organizations and their systems. All DoD information systems must undergo the RMF process to achieve an Authorization to Operate (ATO).

Fortunately, you have a trusted provider that is developing a tool, CSAR, to support the process, and has the expertise to help you along your RMF/ATO journey.

Ingalls provides RMF/ATO Support throughout the RMF Lifecycle with a tailored approach for services.

ATO Support Can Provide:

- ✓ Dedicated support throughout RMF Lifecycle
- ✓ IAM Level III and II Certified Information System Security Manager (ISSM)
- ✓ IAT Level II and III Certified Information System Security Officer (ISSO)
- ✓ eMASS Data Entry and control responses
- ✓ RMF Expert to liaison with Authorizing Official (AO) Staff or Security Control Assessor (SCA)
- ✓ Development of core documentation and evidence
- ✓ Development of RMF/ATO tasks with Project Schedule

You can select from one of our many offerings:

Risk Management Framework (RMF)/Authorization to Operate (ATO) Support

Ingalls will provide a Subject Matter Expert (SME) to provide DoD Risk Management Framework (RMF) Support for Assessment and Authorization (A&A) package for your information systems. The RMF/ATO expert will provide services in designing and implementing information assurance architecture and security controls for the system, or system component, for use within a network or data center environments either on premise or in the cloud. In addition, the RMF/ATO expert provides hands on support in the DoD RMF steps necessary to obtain an ATO.

Information System Security Manager (ISSM)

Ingalls will provide a Subject Matter Expert (SME) to provide DoD Risk Management Framework (RMF) process development for Assessment and Authorization (A&A) package for information systems. The ISSM designs, develops, implements, and integrates information assurance architecture, system, or system component for use within a data center, network, and enclave environments either on premise or in the cloud. In addition, the ISSM participates in information systems risk assessments and designs security countermeasures to mitigate identified risks.

Information System Security Officer (ISSO)

Ingalls will provide a Subject Matter Expert (SME) to provide DoD Risk Management Framework (RMF) support for the ISSM assigned to information systems. The ISSO will assist the ISSM in meeting their duties and responsibilities.



3D Cybersecurity Data Visualization

Our Viewpoint™ software is a U.S.-patented, network security monitoring and correlation system that provides a three-dimensional (3D) visualization of network traffic overlaid with security alerts and other relevant discrete data. This innovative technology gives security professionals the ability to see and interact with data spatially, eliminating the need to scroll through massive spreadsheets of technical data. This quantum leap forward in cybersecurity data visualization provides capabilities that have never existed before.

Trusted partnership. Cybersecurity peace of mind.

Founded in 2010, Ingalls provides cybersecurity consulting, testing, managed detection, and incident response. Having provided incident response services for some of the largest known breaches, we operate with the highest degree of integrity, discretion, and professionalism. Our purpose is to establish Louisiana as a cybersecurity center of excellence, and bring 5,000 industry jobs into the state.



Ready to advance your cybersecurity capabilities? Let us help. Call Government Programs at (888) 860-0452.

DUNS: 03-458-6431

CAGE: 6v7z8

USA Codes/NAICS

Primary - 541512

Information Technology

511210

Software Publishers

517919

All Other Telecommunications

518210

Data Processing, Hosting, and Related Services

541330

Engineering Services

541490

Other Specialized Design Services

541511

Custom Computer Programming Services

541513

Computer Facilities Management Services

541519

Other Computer Related Services

541611

Administrative Management and General Management

541714

Research and Development in Biotechnology (except Nanobiotechnology)

541715

Research and Development in Physical, Engineering, and Life Sciences (except Nanotechnology and Biotechnology)



Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111

WWW.IINFOSEC.COM
(888) 860-0452