

# CYBERSECURITY PRACTICE



Cybersecurity is a challenging problem for government organizations. From ransomware to zero-day attacks, public institutions are under a constant barrage of new cybersecurity threats. Plugging security vulnerabilities can often feel like playing whack-a-mole. More and more everyday devices are Internet-enabled. The new Internet of Things (IoT) includes everything from smart watches to pace-makers. CIOs are facing a larger attack surface than ever before. Navigating these complex challenges requires highly experienced people, mature processes, and powerful toolsets. Here is how IntelliDyne can help.

The unfortunate truth is that exploitation is inevitable. No system is 100% secure. How well prepared is your organization to respond to an incident? IntelliDyne's security operation services provide peace of mind by monitoring our client's network and endpoints for active attacks. Our security operations team provides 24/7 monitoring and incident response. IntelliDyne's managed security services allow CIOs to focus on achieving mission-critical priorities, knowing that we have their back.

IntelliDyne recognizes that cybersecurity is about risk management. The most secure server in the world could be disconnected, placed in an air-tight container, and sunk to the bottom of the ocean – but how practical would that be? System management decisions have to weigh the operation necessity against security risk. At IntelliDyne, we understand this paradigm. Our cybersecurity philosophy is to provide clear and transparent data on risks and solutions, so CIOs can make the best decision for their organization.

---

At IntelliDyne,  
cybersecurity is our passion.  
We provide  
highly experienced  
cybersecurity experts and  
consultants to tackle the  
government's biggest  
security challenges.  
Our team has deep  
experience in cybersecurity  
policy, security operations,  
risk management and  
governance. Our consultants  
are certified with  
industry-leading credentials.

---



## CAPABILITIES

- Assessment and Authorization (A&A)
- Risk Management
- Security Operations
- Security Governance
- Disaster Recovery and Contingency Planning
- Policy Consulting
- Regulatory Compliance
- Vulnerability Management
- Security Automation
- Incident Response
- Network Monitoring
- Spillage Handling



## IMPACTS

- Reduced Risk
- Improved Customer Satisfaction
- Reduced Attack Surfaces
- Improved Compliance
- Fewer Vulnerabilities
- Better Mitigation Strategies

## PROVEN SUCCESS AT DHA

Since 2001, IntelliDyne has provided security operations services for the Defense Health Agency (DHA). We actively monitor thousands of devices for security vulnerabilities and active attacks. Every year, we stop hundreds of attacks and patch thousands of vulnerabilities.

IntelliDyne's risk management team manages the Risk Management Framework (RMF) accreditation for several of the DHA's largest systems and networks. DHA systems under IntelliDyne management have achieved continuous Authorities to Operate (ATOs) for the past decade. DHA sites managed by IntelliDyne have been recognized with "Excellent" ratings on multiple Command Cyber Readiness Inspections (CCRIs).

## ABOUT INTELLIDYNE

IntelliDyne, LLC is a market-leading Government Information Technology firm enabling better mission performance through innovative technology solutions. We manage public sector programs that deliver higher operational efficiency and measurable value to clients. We advise, develop, and execute effective solutions in IT Infrastructure Management, Automation, Analytics, Cybersecurity & Information Assurance, Application Development, and Cloud Computing. **Learn more at [intellidyne-llc.com](https://intellidyne-llc.com).**