

Transformation begins **now**

NGEN Service Management,
Integration & Transport
Quarterly Value Report

FEBRUARY 2022



At Leidos, our mission is to make the world safer, healthier, and more efficient through technology, engineering, and science. And everything we do is built on a commitment to do the right thing for our customers, our people, and our community.

Our deep expertise in mission-focused solutions accelerates our customers' digital transformation objectives. Each day, our global team delivers resilient enterprise IT solutions and managed services at speed and scale that leverage trusted AI, zero trust principles and full-spectrum cyber to decrease burdens and vulnerabilities in complex IT operations. Digital modernization and transformation is a continuous process.

Leidos understands the challenges faced in digital modernization and we bring unique insights to address and tackle some of the most critical roadblocks. We've collected ten key challenges government entities face in digital modernization, along with some insights into how we intend to address and tackle some of the most critical roadblocks. I encourage you to read the full article [here](#).

As your Next Generation Enterprise Network (NGEN) Service, Management, Integration and Transport (SMIT) service provider, we will leverage that digital modernization expertise to improve network operations and introduce new and expanded capabilities to the 650,000 uniformed and civilian professionals who depend on the Navy Marine Corps Intranet (NMCI), the OCONUS Naval Enterprise Network (ONE-Net), and the Marine Corps Enterprise Network (MCEN) for daily IT services.

We're bringing network transformation and modernization to the forefront and developing a five-year transformation plan. We're applying our best practices and proven expertise to a set of candidate initiatives that will modernize and converge the Naval Enterprise Networks. In the coming months, we'll begin moving out jointly with the Department of the Navy on multiple candidate initiatives, as well as continuing the efforts on our Network Operations (NetOps) and service desk contractor-proposed solutions. Our NetOps improvements will enhance enterprise visibility and create a single pane of glass for network operations, while the modernized IT service management tools will provide enhanced customer service.

With the network transitions firmly behind us, we have already completed several key initiatives that are having a positive impact to end user productivity and on your ability to meet mission requirements. Included in this report are project and program highlights designed to keep you up-to-date on what is happening on the SMIT contract, as well as other Leidos projects that I think you'll find relevant.

I welcome your feedback on how you think we're doing and encourage you to email or call me anytime.

D LeGoff

Didier "DJ" LeGoff

VICE PRESIDENT, NGEN SMIT DIVISION MANAGER

619-201-7027

Didier.a.legoff@leidos.com





Table of Contents

- 04** NGEN-R Service Management, Integration and Transport
- 05** Leidos team leverages Model Based Systems Engineering to enhance SMIT performance
- 05** Leidos debuts on Forbes' Best Employers for Veterans 2021
- 06** Leidos completes transition milestone for NGEN-R SMIT
- 06** JADC2 is the future of joint warfare
- 07** Leidos restores connectivity in Indian Head after flooding
- 07** Leidos provides critical support during Tropical Storm Elsa and Hurricane Ida
- 08** Leidos accelerates cybersecurity
- 09** Leidos becomes an AWS Managed Security Service Provider launch partner
- 09** Leidos team propels Navy to Flank Speed
- 10** Training for the return of undersea warfare
- 10** Leidos keeps the Navy's access to Flank Speed moving at, well, flank speed
- 11** The rise of AI at sea
- 11** Leidos ensures vital pier connectivity to the fleet
- 12** U.S. Air Force selects Leidos for counter-small unmanned aerial systems contract
- 12** Leidos supports the U.S. Navy as it participates in Large Scale Exercise 2021

NGEN-R Service Management, Integration and Transport

NEXT GENERATION ENTERPRISE NETWORK (NGEN) SERVICE, MANAGEMENT, INTEGRATION AND TRANSPORT (SMIT)

SMIT provides secure end-to-end information technology (IT) services to more than 650,000 uniformed and civilian professionals who depend on the Navy Marine Corps Intranet (NMCI), the OCONUS Naval Enterprise Network (ONE-Net), and the Marine Corps Enterprise Network (MCEN) for daily IT services.

The SMIT contract was designed with network transformation and modernization as a top priority, a key component in the Department of the Navy's (DON) network modernization efforts, to provide Sailors, Marines and the civilian workforce the tools they need to be more efficient at increasing Naval capabilities – and further empowering the Navy Marine Corps team to compete and win.

The NGEN-R End User Hardware (EUHW) contract was awarded on Oct. 8, 2019 to HPI Federal LLC, and supplies end-user computing and peripheral devices to Navy and Marine Corps users.

SMIT services fall into three main categories:



SERVICE MANAGEMENT

Planning and execution of services and management functions needed to deliver the network and provide mechanisms to resolve incidents, acquire new services, validate changes to services, and receive training on new offerings.



SERVICE INTEGRATION

Integrating interdependent services executed by multiple service providers, orchestrating delivery of end-to-end services to customers, and focusing on core IT services such as the enterprise service desk.



TRANSPORT SERVICES

Planning, provisioning and sustainment of the physical network and the management and optimization of end-to-end transport.

Providing mission critical services across three network domains



Navy Marine Corps Intranet (NMCI)

NMCI is a secure IT platform for more than 500,000 Sailors and civilians at more than 2,500 locations in the continental United States and Hawaii.



Marine Corps Enterprise Network (MCEN)

MCEN is the Marine Corps' network-of-networks and approved interconnected network segments. It comprises people, processes, logical and physical infrastructure, architecture, topology and cyberspace operations.



OCONUS Naval Enterprise Network (ONE-Net)

ONE-Net is the unified computing environment that provides critical connectivity to OCONUS Navy shore commands such as Naval Support Activity Bahrain, home to U.S. Naval Forces Central Command and United States Fifth Fleet.

NGEN-R SMIT combines the support previously provided by the **ONE-Net** and **NGEN** contracts and streamlines service delivery across all three domains



ONE-NET

- Enterprise Service Desk
- Network support



NGEN

NMCI

- Network Operations and IA
- Service Desk and Field Services
- Engineering
- Project Management
- End user hardware

MCEN

- Service Desk support



NGEN-R SMIT

ONE-NET

- Enterprise Service Desk
- Network and IA support
- Field Services support

NMCI

- Network Operations and IA
- Service Desk and Field Services
- Engineering
- Project Management

MCEN

- Service Desk support



NGEN-R EUHW

EUHW

- End user hardware for NMCI, MCEN and ONE-NET



Network Operations

650,000
Users Supported

28,000
Network Devices



Security Operations

450,000
Endpoints
Scanned/Patched

500+
Digital Forensics
Investigation/Year

400+
Sensors

2,500
Site Locations

453,000
Seats Serviced

1,100
VTC Devices

55,000
Printers

125,000
Service Desk Interactions/Month

Leidos team leverages Model Based Systems Engineering to enhance SMIT performance

The Leidos Next Generation Enterprise Network (NGEN) Service, Management, Integration and Transport (SMIT) team is taking a fresh approach to how engineering services are delivered, resulting in enhanced program performance. Specifically, within the SMIT Engineering space, Leidos is using model-based systems engineering (MBSE) to develop requirements, architecture, and design. The MBSE engineering practice is just one part of Leidos's overall SMIT network transformation and modernization effort.

MBSE allows organizations like the SMIT engineering team to get a visual representation of the system they're working on, making it easier for them to visualize system interdependencies. MBSE is an agile approach that uses model development, reuse, and integration methods to help teams quickly respond to evolving systems engineering needs. The well-defined MBSE methodology also provides the opportunity to enhance productivity, innovation, communication, and quality, while also reducing risk. For the Leidos SMIT team, MBSE also enhances our ability to create and manage multiple baselines, leverage automated configuration management, assess interdependencies, and provide rapid evaluation of performance and interoperability impacts.

Our SMIT team is leveraging Leidos' MBSE Center of Excellence (CoE), enabling us to offer this capability at scale. The MBSE CoE supports the SMIT team through centralized program support, focus on adoption and transition, and developing enterprise maturity. This leads to a proven digital engineering approach that replaces labor-intensive, document-centric processes, and allows the engineering teams to focus their efforts on the most vital engineering tasks. The Leidos MBSE tools are not just model-centric; they can support the entire lifecycle of an engineering program.

Because the data is related digitally, solutions, ideas, and processes can be quickly understood, and associations identified more efficiently. Engineering analyses such as trade studies, requirements management, performance modeling, interface definition, verification, and impact analysis are analyzed, developed, and deployed more efficiently to any project stakeholder, both internally and externally.



Leidos debuts on Forbes' Best Employers for Veterans 2021

Leidos debuted at No. 90 on [America's Best Employers for Veterans 2021](#), published by Forbes.

Leidos ranks in the top ten in the IT, Internet, Software & Services category. It's the company's first year on the list, which is in its second running.

WHY YOU SHOULD KNOW

Roughly 200,000 veterans transition from military service to the civilian workforce every year, [according to the Labor Department](#). Companies on the list and many others are committed to supporting veterans and their families in this transition.

METHODOLOGY

The list, powered by [Statista](#), ranks the top 200 U.S. companies with more than 100 employees that veterans in the workforce like best.

"To determine the list, Statista surveyed more than 5,000 American veterans who have served in the U.S. armed forces, either in the regular military or in the National Guard or military reserves," according to its publishers.

It's based on criteria that measure an employer's "working conditions and approach to diversity and inclusion, as well as whether their environment is veteran-friendly."

Other criteria include salary and wage, image, and atmosphere and development.

THE DATA SAYS

Leidos employs nearly 8,500 veterans, who represent 20% of the company's workforce, including roughly 2,200 disabled veterans.

FROM THE SOURCES

"Hiring and supporting military veterans and their spouses is a core component of both our company's values and strategic plan," said [Leidos Defense Group](#) President Gerry Fasano. "We are humbled to have been selected as one of America's Best Employers for Veterans and look forward to strengthening our long-standing commitment to those who have bravely served our country with honor and distinction."

"Veterans bring training, experience and oftentimes certifications which are requirements for many of our positions," says Alex Verhulst, head of the company's [veteran outreach program](#). "They're familiar with the fast-paced environment and mission-oriented culture of our organization and have the best mindset and work ethic for putting mission execution and success first."

It's the latest in a series of major recognitions for Leidos, which also ranks as one of America's [most female-friendly companies](#), [most ethical companies](#), [most admired companies](#) and [best employers for diversity](#).

In 2021, Leidos was named a Military Times [Best for Vets Employer](#) for the eight consecutive year and was a first-time recipient of the U.S. Department of Labor's [HIRE Vets Medallion](#).



Leidos completes transition milestone for NGEN-R SMIT

The Leidos SMIT team has completed the transition for the Department of the Navy's Enterprise IT networks. The effort represents the foundation for the broader IT modernization planned under the Service Management, Integration and Transport (SMIT) contract that was initially awarded in February 2020 as part of the Next Generation Enterprise Network Recompete (NGEN-R).

On August 1, the Leidos team assumed responsibility for the end-to-end IT operations for the Navy-Marine Corps Intranet (NMCI) and the OCONUS Naval Enterprise Network (ONE-Net), as well as support for the Marine Corps Enterprise Network (MCEN). Combined, the three networks provide IT services for more than 650,000 uniformed and civilian professionals who use it daily in more than 1,500 locations across the U.S. and worldwide.

"Ensuring the Navy has an agile and responsive network is critical to national security, and we are proud to complete the transition successfully," said Dan Voce, Senior Vice President and Enterprise & Cyber Solutions Operations Manager for Leidos. "With this contract, the Navy is moving closer to

enterprise networks that can more rapidly develop, test, and deploy new mission-critical technologies while maintaining the highest levels of cybersecurity."

In February 2020, Leidos was awarded the NGEN-R SMIT contract, valued at \$7.7 billion over 8 ½ years. After a series of contract protests, Leidos received the formal go-ahead to begin the transition in February 2021. The Navy and Leidos worked together to accelerate the transition timeline from nine months to six months; with the final phase of the transition completed on August 1.

As part of the modernization efforts expected by the Navy, the Leidos team will focus on using innovative technologies to support improved network operations and foster quicker development, testing and deployment of new IT solutions.

"We are excited to complete our transition and start improving operations," said Didier LeGoff, Leidos division manager for the SMIT contract. "SMIT's success will be measured by how well the Navy can leverage smart, scalable networks while addressing future warfighting challenges. Leidos is ready to help the Navy meet and exceed that standard."



JADC2 is the future of joint warfare

The future of joint warfare — missions in which two or more military branches team together — rests on a new operational imperative called Joint All-Domain Command and Control (**JADC2**), an ambitious plan to synchronize digital technology together across branches.

Why you should know: While joint operations are common, there's often limited connectivity between U.S. military branches when it comes to their sensing and shooting technology.

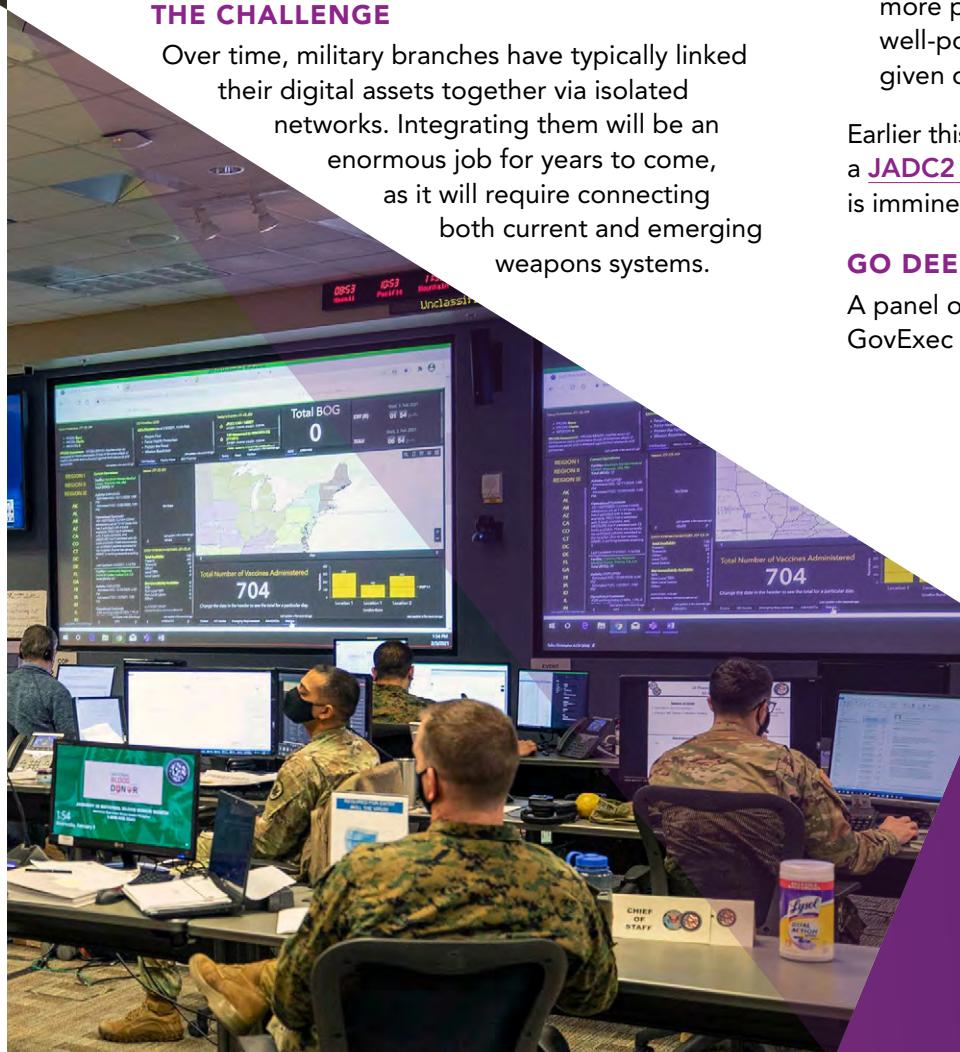
A peer adversary with greater interoperability across its forces **would have an advantage** in a war against the U.S.

JADC2 will link sensors and shooters across service branches and domains through a shared network, which military leaders believe will improve awareness, decision making, and response times on the battlefield.

► For example, if a Navy airplane senses an enemy threat, JADC2 framework will enable the pilot to respond using Army artillery and Air Force cyber weapons simultaneously.

THE CHALLENGE

Over time, military branches have typically linked their digital assets together via isolated networks. Integrating them will be an enormous job for years to come, as it will require connecting both current and emerging weapons systems.



FROM THE SOURCES

► "JADC2 is not a single platform, but a warfighting concept of digitally connecting the joint force across air, land, sea, cyber and space domains," said Chad Haferbier, a Leidos Vice President leading the company's JADC2 efforts. "The Department of Defense recognizes that data is the new high ground, making the ability to securely share data across the force key."

► "JADC2 aims to close the decision loop and accelerate the military's ability to rapidly address a threat," said Leidos expert and retired Brigadier General J.B. Burton. "Simply put, JADC2 will make our joint warfighters more effective by equipping them with the best information as quickly as possible to conduct operations around the globe."

► "The military Internet of things has arrived," says Leidos expert Erik King. "Fifteen years ago, we could conceive of it, and the technology was there, but now the maturity of that technology has made advanced sensors and the accumulation of data far more prevalent. Industry partners like Leidos are well-positioned to support the military on JADC2 given our military systems integration expertise."

Earlier this year, Defense Secretary Lloyd Austin signed a **JADC2 strategy**. A classified implementation plan is imminent, according to **reports**.

GO DEEPER

A panel of Leidos experts recently sat down with GovExec to discuss **five key drivers of JADC2**.

Leidos restores connectivity in Indian Head after flooding

The Leidos SMIT team recently demonstrated the power of teamwork in their response to an incident at the Naval Surface Warfare Center (NSWC) Indian Head (IHD) in Maryland. In the early morning hours on Sunday, Aug. 8, 2021, an underground pipe carrying water for the fire suppression system burst and flooded a building on NSWC IHD. Over the next several hours the broken pipe pumped water through the building's concrete slab and into multiple areas: a Marine Corps warehouse, the NMCI field services office and the Installation Service Node (ISN), which provides IT services to nearly 3,000 NMCI users located on the base.

While the Leidos NMCI Network Operations team transitioned NMCI services to an alternate server farm, the local Leidos field services and data center teams arrived shortly after being notified and were able to power down all the equipment to prevent further damage. "When we arrived, we found nearly a foot of mud and water in our field services office and in the server farm," said Trent Helms, NGEN SMIT facilities manager. "Administrative and ISN equipment was submerged, rendering the base transport boundary inoperable."

After creating a comprehensive inventory of equipment that would have to be replaced before full local NMCI services could be restored, the team vacated the space to allow for dewatering and a thorough cleaning. The Navy gave Leidos the approval to return to the ISN late Thursday afternoon and within six hours of arrival, the teams had replaced all of the damaged equipment and were able to partner with network services to bring local connectivity back online.

In addition to quick thinking and teamwork, the key to Leidos' success was the ability to quickly pull the required replacement parts from existing inventory in Mechanicsburg, Pa. "Everyone truly came together to quickly react to the situation, even as they were knee deep in transition," said Data Center Operations Leader James Bingham. "Matt Willing, the asset management manager, even drove the equipment down from Mechanicsburg."

As a field activity of the Naval Sea Systems Command, and part of the Navy's Science and Engineering Establishment, NSWC IHD is the Navy's premier facility for ordnance, energetics and explosive ordnance disposal solutions. When the military experiences problems with current weapon systems or encounters new threats on the battlefield, NSWC IHD answers the call to provide the solution.

Leidos provides critical support during Tropical Storm Elsa and Hurricane Ida

When the winds and rains of recent Tropical Storm Elsa and Hurricane Ida threatened connectivity and support to the Navy and Marine Corps this summer, the Leidos SMIT team charged into action. Tropical Storm Elsa made landfall in Florida and New England in early July, and Hurricane Ida made landfall in Louisiana in late August.

Before a storm makes landfall and throughout their path, the Leidos SMIT Business Continuity, NMCI Network Operations Center (NOC) and Marine Corps Enterprise Network (MCEN) teams carefully monitored the storm tracks to ensure they were prepared to take necessary actions.

"Our incident response protocol is to monitor any potential impact to the NMCI network and users," said Jack Cullen, SMIT IT service continuity lead. "Once we determine the potential for impact, we enact our critical situation mitigation protocols." Those mitigation protocols include the accountability and safeguarding of all employees, equipment and services that support the SMIT contract.

Prior to a storm's arrival, the team also determines facilities and services in the storm's path that may need to be rehomed, migrated, or failed over to a safe location to ensure users remain connected to as many services as possible during such a critical time. "While both Elsa and Ida were large and powerful, neither of them impacted any NMCI sites that hosted

vulnerable NMCI servers or services," said Jack. "Had Elsa hit further south in the area of Norfolk, Va., a major effort would have been initiated to migrate those NMCI assets and services at another location."

While the Navy's largest base was spared during the 2021 hurricane season, the Marine Corps Support Facility New Orleans found themselves directly in Hurricane Ida's path. The storm caused network connectivity issues at the Marine Corps Forces Reserve (MARFORRES) site. Leidos team members remained on base at the MCEN facility overnight to provide network operations, administration and IT support. The team members worked around connectivity and telephone disruptions and no air conditioning in the sweltering bayou temperatures. At the same time, some team members were relocated to Fort Worth, Texas, a designated safe space serving as temporary MARFORRES headquarters. These team members acted quickly and were ready to travel on short notice, some staying for almost two weeks supporting the customer remotely. Many pivoted quickly to continue providing tech support to staff that were at remote locations.



Leidos accelerates cybersecurity

The term “accelerate” is defined by Merriam-Webster as “to move faster; to gain speed.” Acceleration implies an object, a project, or even an idea that was already moving at some pace, picks up even more forward momentum through focused effort and energy. Leidos has borrowed this word and applied it to a small number of our most critical and fast-moving business segments, including artificial intelligence (AI) and, most recently, cybersecurity. In June of 2021, **Meghan Good**, VP and Technical Fellow, was tapped to lead the critical new internal group of cyber experts we call the **Leidos Cyber Accelerator**. With nearly 20 years of experience in various cybersecurity and intelligence positions, Meghan has already shown energetic leadership and enthusiastic technical expertise leading this group to several significant wins in the competitive landscape.

But what is an accelerator anyway? We sat down with Meghan to ask questions like this one and get her perspective on her new role. Meghan explained, “An accelerator, and in this case, the Cyber Accelerator represents a focal point of technology development where we look at customer challenges across the company and pull from many different sources looking for rapid ways to solve these problems.” The concept of accelerators, in general, is not unique to Leidos. In fact, similar concepts can be found in startups and tech companies all over the world. The difference is that as a diversified, major technical contractor Leidos has access to brainpower that simply may not be available to businesses of a smaller size who are still looking for steady revenue streams. “Whether it’s

research from the academic world, external partners, input directly from customers at the highest levels of government, or our own research and development, Leidos’ Cyber Accelerator pulls from these centers of knowledge and is able to scale new solutions at a pace that is really impressive,” she added.

While technical expertise and deep knowledge of the cyber world is crucial to operate a successful accelerator, developing a keen eye for multidisciplinary talent may be equally as important. The Leidos Cyber Accelerator is staffed differently than other parts of the company. Rather than building teams around one or two central subject matter experts in a given line of business, the Cyber Accelerator seeks to pull from all talent pools, creating a diverse team that is motivated to challenge conventional thinking. In addition to prioritizing innovation and ingenuity, getting solutions to customers fast has to be front of mind in an accelerator environment. Meghan said about the need for a multidisciplinary team, “It’s actually one of my favorite parts of the job. I get to think creatively and look for people with different experiences. If they’re energetic, talented, and ready to take on serious challenges, I can find a home for them here.”

As the name implies, speed and focus are essential themes for a business unit like the Cyber Accelerator. But what more specific goals are the Cyber Accelerator looking to accomplish? It’s clear that cyber challenges are here to stay, and bad actors are becoming more sophisticated and brazen than



A professional portrait of Meghan Good, a woman with dark, curly hair, wearing a dark blazer over a light-colored top. She is smiling and looking directly at the camera. The background is a solid grey.

ever before. What is the Cyber Accelerator working on now to address the threat? “Without getting into specifics, a lot of what we’re working on lately has to do with advanced analytics and finding new ways to counter advanced threats. We’re really looking hard at the intersection of cyber operations and machine learning, or other forms of **AI (artificial intelligence)**. We’re also very focused on what it’s going to take to bring a **Zero Trust** philosophy into the real world in terms of implementation,” Meghan said. With these goals in mind, Leidos stands out as a clear leader as some of these technology areas like AI/ML and Zero Trust are already fully staffed Leidos operations being researched and worked on by Meghan’s colleagues. In fact, AI/ML is the focus of another Leidos Accelerator led by a peer Leidos Technical Fellow of Meghan’s, Ron Keesing. Check out our recent podcast, **Can AI be trusted?**, that features Ron. Did we mention that Meghan is also the co-host of the **MindSET** podcast?

Anyone who pays attention to the news can see that the need for enhanced cyber protection is real. And to closer observers, it’s clear that the tradecraft cyber attackers employ is getting more complex and more sophisticated all the time. That’s all to say that the demand for state-of-the-art cyber technology efforts like the ones the Leidos Cyber Accelerator develops exists in spades. Put more simply; the need is there for Meghan’s team’s work. But it’s one thing to know that you’re needed. It’s another thing to feel passionate and excited about the work. “My background is as a Cyber Threat Intel Analyst, so for me, I want to improve detection, to analysis, to action and making that cycle run fast enough and reliable enough that we can really make a difference.” She added, “We’ve added so much complexity to our environments that visibility and control can be

challenging to maintain. Anything we can do to improve that so we’re making intelligent decisions faster is really exciting to me.”

With a pedigree as interesting as it is impressive, Meghan is truly dedicated to Leidos’ important work. In fact, Meghan has spent the entirety of her career with Leidos, having started with the company as an intern during her years as a computer science undergrad at Boston University. That kind of loyalty is certainly rare these days, especially with the high demand for cyber talent in both the public and private sectors. After completing her internship and earning both a bachelor’s and then a master’s degree from BU, she rejoined Leidos and held several roles in the cyber arena, including acting as the Cyber Solutions Lead, Solution Architect and even spent some time in a marketing role after completing her MBA at the University of Maryland. Today, in addition to being a supportive and effective manager and leading the new Cyber Accelerator, she also has her research responsibilities as a technical fellow, where she focuses on bringing data visualization models to the cybersecurity world. “One of the biggest challenges in cybersecurity is communication. We communicate very technical indicators to non-experts and expect them to make significant decisions without much context,” she said. “I think we can communicate better using graphics, but we need them in real-time. I’m working on a series of analytics that builds data-rich visualizations to provide necessary context, but not too much information to overwhelm decision-makers.”

Leidos becomes an AWS Managed Security Service Provider launch partner

As the world becomes more dependent on cloud-based solutions and services, we recognize the importance of being a leading innovator in this rapidly evolving market. The company's partnership with Amazon Web Services (AWS) Partner Network (APN) as a [Premier Partner](#) is key to this effort, and the thriving relationship between Leidos and AWS is evident in the recognition Leidos has achieved. Since joining the AWS Partner Network in August 2014, Leidos has been selected for various competencies and programs.

Most recently, Leidos achieved AWS Level 1 Managed Security Service Provider (MSSP) competency status. This designation recognizes that Leidos is at the forefront of the managed security services field. It showcases that the company offers a demonstrated capability – providing customers with a mature baseline of managed security services to protect and monitor customers' essential AWS resources around the clock. AWS introduced this standard of quality for managed security services to benefit cloud environments of any size. It spans six security domains: vulnerability management, cloud security best practices and compliance, threat detection and response, network security, host and endpoint security, and application security. The six domains contain multiple MSSP services, each with technical skillset and operational process requirements specific to AWS.

Leidos' footprint with the AWS Partner Network extends beyond this most recent recognition. Beginning in April 2018, Leidos holds the AWS Managed Service Provider certification. This certification, which is reviewed annually, identifies Leidos as a mature and well-managed cloud service provider. It also reinforces to customers that Leidos has the ability to plan, design, build, migrate, run, and optimize complex systems hosted in AWS cloud environments. As the relationship between Leidos and AWS continues to develop and thrive, Leidos demonstrates the AWS connection in each of its core business and technology areas.

Leidos has achieved the AWS Government Competency certification for multiple industries, including national security and defense, citizen services, and public healthcare. In 2020, Leidos earned the AWS Healthcare Competency and the AWS Migration Competency. The healthcare competency demonstrates the company's expertise in the specific performance, reliability, and data protection requirements of the healthcare industry. The migration competency is a "horizontal competency," in which Leidos used reference programs to demonstrate the ability to migrate customer's systems to the cloud.

Another way Leidos continues to make an impact with AWS is through its role as a long-time sponsor of the AWS Public Sector Summit – held annually in Washington D.C. This year, the company is a Platinum level sponsor.

These achievements served as stepping stones to obtaining and maintaining Leidos' status as an AWS Premier Consulting Partner. This designation, which the company has held since June 2018, is the highest tier within the APN and is awarded by an executive committee within AWS. It recognizes partners who are market leaders, proven innovators, and who have made significant investments in technical skills and AWS expertise to drive successful customer outcomes.

Leidos' teams are confident that the partnership between Leidos and AWS will continue to flourish. From AWS account creation to active security maintenance in production, Leidos' security processes and design approach provide secure and operational systems in the cloud. The company's security-centric mindset and culture of continuous innovation ensures solutions align with and exceed AWS and industry best practices. As an AWS Managed Security Service Provider (MSSP) Competency launch partner, Leidos leads the industry in providing customers with secure, well-managed AWS cloud environments.

Leidos team propels Navy to Flank Speed

Together with the Navy Flank Speed team, the Leidos SMIT team recently migrated more than 214,000 NMCI users to the Navy's Flank Speed cloud. Flank Speed is a single Microsoft Office 365 (M365) collaboration and productivity environment designed to improve security and provide for a more productive Navy workforce.

To ensure the migrations were as seamless as possible to end users, the Leidos service desk teams provided assistance to users configuring their accounts for migration to Flank Speed. In addition, the service desk provided a separate "VIP" support team to assist with the VIP transitions in the Pentagon and other senior executive operations.

Named after the extreme engine order given to ship handlers to evade danger or outpace threats, Flank Speed will be an evolving information technology initiative and the epicenter of Navy unclassified systems for years to come.



Training for the return of undersea warfare

Thanks to a major submarine deal between the U.S. and Australia [announced last month](#), along with the growing Chinese threat, submarine fighting is top-of-mind in the public for the first time since the Cold War.

But submarine fleets have proliferated around the world for some time:

- Six nations now operate modern nuclear subs, according to [Foreign Policy](#).
- Brazil and Australia will soon [join the list](#).
- China will likely maintain between 65 and 70 submarines [over the next decade](#), although many are non-nuclear.
- Russia also [continues to grow](#) its submarine fleet.

Quieter and more capable than their Cold War predecessors, enemy submarines pose a far greater threat. They can sink warships and strike targets on land more effectively, posing a major threat in the western Pacific and beyond. Leidos is helping the Navy modernize the training process to detect them.

THE CHALLENGE

Anti-submarine warfare (ASW) starts with knowing what lies beneath the surface, making sonar technology an integral part of the Navy's self-defense.

But the physics of underwater sound are complex. Sonar technicians need specialized training to find, classify and track submarines.

THE SOLUTION

The Navy launched a new [virtual training system](#) that decentralizes its training program, reducing costs and increasing efficiencies over a single training location. The virtual tool mimics the warfighter's equipment, providing additional opportunities to practice their ASW skills in realistic underwater environments.

FROM THE SOURCE

"The hardware virtualization is an economical solution that the Navy can utilize in classrooms around the world," says Dan Newell, a Leidos expert in undersea surveillance. "The realism, accessibility and limited footprint of the simulation help support Sailor readiness."

Newell's Training Systems Engineering Team (TSET) and the Leidos Modernization Training Support Team (MTST) supported the project.

ZOOMING OUT

"The Soviet strategy during the Cold War was to overwhelm their adversaries with numbers, not capability," Newell said. "That's now changing, so we must increase our ASW capability to pace the threat and improve detection and accuracy. Today's Sailors need new skills and focus, and solutions like these virtualized tools will help them succeed in tomorrow's high-end fight."

The system [launched in the spring](#) and will expand later this year. More than 2,000 Sailors have been trained using the new system and its prototypes since 2018.

Leidos keeps the Navy's access to Flank Speed moving at, well, flank speed

When routing issues recently caused some NMCI users to experience a slow Flank Speed connection experience, the Leidos SMIT team jumped in to get them back to moving at, well, flank speed.

NMCI network traffic that is bound for the cloud is typically routed through the DISA Secure Cloud Computing Architecture (SCCA) Boundary Cloud Access Point (BCAP). The access point serves as a network connection point for the many cloud express routes from the network.

While investigating the Flank Speed latency reports, the Leidos team quickly discovered that a project done on the previous contract intended to increase network speed had inadvertently routed some NMCI cloud traffic through a small server farm in California.

The extra traffic overloaded the server farm and slowed user attempts to connect to the cloud and to the Navy's Flank Speed. Flank Speed is a single Microsoft Office 365 collaboration and productivity environment designed to improve security and provide for a more productive Navy workforce.

"Once we identified the issue, we were able to quickly determine a solution and submit the proposal to the government that would allow us to re-route that traffic through the appropriate BCAPs," said Heather Tipton, Unified Communications and Cloud Architect. "We implemented the change as soon as the Navy gave us the green light."

This type of quick problem resolution is exactly what the Navy can expect from Leidos team as they pivot the network toward much needed modernization. "I'm proud of the way the team came together to both investigate and solve the issue in a timely manner," said Christina Turek, Leidos NMCI program manager. "The Navy's modernization strategy directly aligns to our core technical capabilities, and I look forward seeing us come together to modernize the network and provide improved services those who count on us every day."



The rise of AI at sea

The Navy wants to [expand its fleets](#) by as many as 89 uncrewed surface vehicles (USVs) over the next several years. USVs use artificial intelligence (AI) in place of a human crew, and are designed to operate autonomously for weeks or months at a time.

WHY YOU SHOULD KNOW

USVs are one of the most promising areas of military AI expansion. They could help the Navy reduce acquisition costs and staffing requirements. More importantly, they could minimize risk to U.S. sailors by operating out in front of the fight.

The Pentagon is funding prototypes and purchasing new ships, including two manufactured by Leidos:

- [Seahawk](#), with a cruising range of several thousand miles and speeds comparable to crewed warships.
- [Sea Hunter](#), which costs a fraction of what a crewed vessel of similar capability would cost.

WHAT THEY CAN DO

USVs are promising alternatives to crewed warships for a range of missions:

- Carrying surveillance payloads
- Hunting mines
- Towing supplies
- Searching for acoustic signals in deep water
- Mapping the sea floor for safe navigation

FROM THE SOURCE

"Right now it's expensive to run some of those missions," said Leidos expert Dan Brintzinghoffer. "You'd probably use a destroyer, which costs a couple billion dollars, and a crew of 300 sailors. You could send a USV instead and be just as effective."

But the technology behind USVs is very different than uncrewed aerial vehicles (UAVs) and driverless cars. Autonomy at sea presents unique engineering challenges.

USVs must maintain themselves for long periods of time, including systems for:

- Propulsion
- Heating and cooling
- Electrical distribution
- Communications

"If you add an algorithm to the navigation system of an existing ship, it might get you from point to point," Brintzinghoffer said. "But what if your engine fails?"

USVs must also comply with [COLREGS](#), the universal instructions to avoid collisions at sea.

Maritime collisions [kill thousands](#) each year. The summer of 2017 alone saw two major collisions involving US destroyers and multiple fatalities:

- The USS Fitzgerald collided with a tanker near Tokyo.
- The USS John S. McCain collided with a tanker near Singapore.

"Most of these accidents happen when someone doesn't do what's expected," Brintzinghoffer said. "USVs must be smart enough to conduct missions within COLREGS or risk self-destruction."

LOOKING AHEAD

While survey and logistics missions are good starting points, Brintzinghoffer said USVs will take on more complex and dangerous missions as the Navy becomes more comfortable trusting them.

As USV technology advances, the Navy can offload routine or dangerous missions onto USVs, options which are safer and less costly.

Earlier this year, Leidos [acquired](#) naval architecture and marine engineering firm [Gibbs & Cox](#) to help the Navy achieve its goals in the maritime undersea, autonomous, and cyber security segments.

"Gibbs & Cox is widely regarded for developing the most talented and experienced naval designers in the world," said Leidos Chairman and CEO Roger Krone. "We look forward to this new era of innovation while combining the best of both companies."

Leidos ensures vital pier connectivity to the fleet

Leidos recently rolled out piers connectivity services as a separate line item on the SMIT contract. The services provide pier side connectivity for U.S. Navy ships in key Navy locations.

When a Navy ship returns to port, the Leidos SMIT team will provide critical connectivity by connecting an umbilical cable assembly (UCA) to the ship. "The UCA is a fiber cable Navy ships use connect their IT systems to the shore side network," said Paul LeBlanc, Leidos Service Delivery Manager for NMCI Transport Services. "When not in use, the UCAs are typically stored locally in a reel and frame and are pulled back out when a ship comes back to port."

Before Leidos could provide this mission critical service, the team had to gain access to Navy piers. To that end, Leidos worked to procure vehicles, execute leasing agreements, and obtain the appropriate clearances and passes that would allow access. "To make sure we were able to continue to deliver this mission-critical service while we worked through the necessary wickets, we partnered with a vendor who had previously offered the service," said Paul. "Together, we worked to pre-stage as many UCAs on the piers as possible."

Under the SMIT contract, the piers connectivity services will be handled through the service desk ticketing system. Additionally, the team is also working to determine the viability of the current government furnished equipment and will recommend replacements where necessary. Pier side connectivity is currently available at ports located in Bangor, Bremerton and Everett, Wash.; Little Creek, and Norfolk, Va.; Mayport, Fla., Pearl Harbor and multiple San Diego locations. Additional CONUS and OCONUS locations will be added in the coming months.



U.S. Air Force selects Leidos for counter-small unmanned aerial systems contract

Leidos has been awarded a prime contract by the U.S. Air Force to support the service's counter-small unmanned aerial system (C-sUAS) efforts. This single-award, indefinite delivery, indefinite quantity contract includes a one-year period, as well as four one-year options. Work will be performed at various CONUS locations.

"The complex and rapid proliferation of small, unmanned aircraft systems by adversaries presents new risks and challenges for our armed forces," said Will Johnson, Leidos Senior Vice President, Logistics and Mission Support. "We are proud to support the Air Force's mission to increase the operational capability of fielded and future C-sUAS equipment."

Through this contract, Leidos will support the Air Force Life Cycle Management Center and enhance the air base defender's capability to detect, identify, track and defeat small Unmanned Aircraft Systems (sUAS). This will take place through a wide range of system and software maintenance, development and deployment tasks. Leidos' innovation and agile technologies will play a critical role in enhancing base security capabilities, while enabling a fully connected defense solution to combat anticipated threats to air bases worldwide.

Headquartered at Wright-Patterson Air Force Base, Ohio, the Air Force Life Cycle Management Center is one of six centers reporting to the Air Force Materiel Command and provides test and evaluation, life cycle management services and sustainment for every major Air Force weapon system.



Leidos supports the U.S. Navy as it participates in Large Scale Exercise 2021

The Leidos SMIT team recently provided critical support to Fleet Cyber Command and Naval Network Warfare Command (NETWARCOM) in their planning and execution of Cybersecurity Response Actions in support of the Large Scale Exercise objectives.

Large Scale Exercise (LSE) is a triennial exercise conducted by U.S. Fleet Forces Command, U.S. Pacific Fleet, and U.S. Naval Forces Europe that is designed to refine how we synchronize maritime operations across multiple Fleets, in support of the joint force. The training is based on a progression of scenarios that will assess and refine modern warfare concepts.

LSE 2021 is the first iteration of what will become a triennial exercise with plans for future iterations to include partners and allies from around the world.

Over the course of the exercise, Leidos directly responded and supported to several technical Requests for Information (RFI) from NETWARCOM to support more than 100 potential cyber security measures and mitigations. "This evolution reinforced that the Navy relies on NMCI to conduct maritime operations," said Chris Malone, Leidos NMCI Cyber Operations. "Our team looks forward to future opportunities to provide such critical support to our clients."



NGEN SMIT
Service Management, Integration & Transport

 **leidos**