

IP and Data Rights: Protecting DoD's Access to Innovation

White Paper

Table of Contents

Executive Summary	3
Introduction.....	4
Current NDAA Right to Repair Proposals	4
Reducing Innovation and Industry Concerns with RTR Proposals	5
Existing and Alternative Solutions.....	6
Current DoD Authorities Available for Data Rights and IP	6
Creative and Surgical Solutions for IP and Data Rights	7
Understanding the Real Challenges of Readiness and IP’s Role	8
Closing	9
Endnotes	10

September 2025

About NDIA

For over 100 years, the National Defense Industrial Association (NDIA) has provided a forum for government and industry leaders to collaborate and address complex defense issues so our nation’s security can maintain a strong, diverse U.S. defense industrial base. NDIA’s and its affiliates’ membership embodies the full spectrum of corporate, government, academic, and individual stakeholders, with over 1,700 corporate members, the majority of which are small businesses, and over 67,000 individual members.

First published in 2025 by NDIA, 2101 Wilson Blvd, Suite 700, Arlington, VA 22201, United States of America. (703) 522-1820

© 2025 by the National Defense Industrial Association. All rights reserved.

This white paper is made possible by general support to NDIA. No direct sponsorship contributed to this report. This white paper is produced by NDIA, a nonpartisan, nonprofit, educational association that has been designated by the IRS as a 501(c)3 nonprofit organization and was founded to educate its constituencies on all aspects of national security. Its research is nonpartisan and nonproprietary.

For more information, please visit our website: [NDIA.org](https://www.ndia.org)

POLICY QUERIES: Mseeds@NDIA.org

MEDIA QUERIES: Media@NDIA.org

Executive Summary

The Department of Defense's (DoD) access to innovation is weakened when companies are at risk of losing sensitive, proprietary intellectual property (IP). The recent "Right to Repair" (RTR) proposals to address sustainment challenges and concerns involving the perception of vendor lock are not the right answer. While presented as a solution to military readiness challenges, proposed RTR mandates misdiagnose the problem and deter companies, including traditional contractors, nontraditional, and small businesses, from both working with the DoD and focusing innovative research on defense applications. A more effective approach to data rights and IP involves understanding and leveraging existing authorities and exploring collaborative alternatives that respect IP while ensuring sustainment requirements are met.

RTR provisions included in the pending House and Senate versions of the Fiscal Year (FY) 2026 National Defense Authorization Act (NDAA) would compel contractors to provide the government with "fair and reasonable access" to all repair parts, tools, and information. This mandate would force the disclosure of companies' sensitive, privately funded IP and trade secrets, which the DoD could then share with third parties, including direct competitors. This approach poses significant risks:

- **Reduces Access to Innovation:** Forcing companies to risk their core IP—the "crown jewel" of their business—will drive them away from the defense market and reduce their defense-focused R&D. An NDIA survey shows 36% of companies have already chosen not to bid on DoD contracts over IP concerns, a 14-percentage-point increase from the previous year.¹ RTR mandates will only accelerate this trend.
- **Forces Disclosure of Proprietary Data:** Compelling the transfer of sensitive technical data and trade secrets weakens a company's competitive advantage. It also increases the risk of reverse engineering and IP misappropriation by domestic or international competitors, as well as potential U.S. adversaries.
- **Increases Legal and Safety Risks:** The government's power to define "fair and reasonable" terms, which is statutory and unilateral government control to determine prices, terms, and conditions, creates contractual uncertainty for prior licensing agreements and third-party integrations. Furthermore, allowing third parties to reverse-engineer and manufacture critical components introduces unacceptable safety risks for military personnel.

Solutions:

Instead of imposing RTR mandates, DoD and Congress should focus on solutions that address real challenges and foster a collaborative environment. For example, at a recent congressional hearing, Under Secretary of Defense for Acquisition and Sustainment Michael Duffey acknowledged the complexity of IP and emphasized the need to be "creative" and "surgical" in how DoD gains access to data "while still respecting the need to protect the intellectual property that's privately funded and is really an engine of the innovation that we are dependent upon."² Fortunately, DoD can address many challenges without requiring legislative change. In addition, there are also provisions pending in the FY26 NDAA process that meet DoD's creative and surgical solutions policy objective:

1. **Fully Utilize Existing Authorities:** DoD already has powerful, flexible, and underutilized statutory tools to negotiate for the specific data rights it needs for sustainment. This includes a statutory requirement for major weapons systems for DoD to contract for the technical data it needs, including any needed for operations and maintenance, up front, which then allows servicemembers to make the needed repairs (see Current Authority Chart on page four).
2. **Inventory Data Rights (Finstad Amendment):** A proposed amendment³ to the House NDAA would require the DoD to inventory the technical data it currently holds for major weapon systems. This would identify actual, specific gaps in data needed for sustainment, allowing for targeted, cost-effective negotiations rather than a damaging, one-size-fits-all mandate.
3. **Implement Data-as-a-Service (DaaS):** This innovative model would allow the DoD to contract for access to a contractor's full technical data library on a "pay-per-use" basis. The DoD could access and use data for a specific repair when needed, ensuring readiness while allowing the contractor to protect its underlying IP from broad disclosure.

Ultimately, the best way to ensure warfighter readiness is for the Department to be a reliable partner that respects IP. This will attract, not deter, the innovative companies and private investment needed to maintain technological superiority.

Current law provides DoD the authority to contract for the technical data needed for servicemembers to make repairs. Future changes should implement creative cost-saving approaches, like Data-as-a-Service, and avoid IP mandates that reduce innovation and deter companies from working with the Department.

Current Authority Overlap of Right to Repair (RTR) Proposals			
	Current Authority	Senate NDA A RTR	House NDA A RTR
Requirement to agree to provide technical data prior to entering into a contract	Yes. 10 USC 4236 currently requires agreement for any technical data prior to selecting a contractor for development, production, or sustainment of a major weapons system.	Yes. Proposed 10 USC 4664(a)(1) for instructions for continued operational readiness (ICOR) for covered defense equipment.	Yes. Proposed 10 USC 4664(a) for repair goods in support of a major weapon system.
License for government employee use of technical data for repairs	Yes. 10 USC 3771 (DFARS 252.227-7013 for Limited Rights) allows the government to use, but not disclose to third parties, privately developed items, components, or processes.	Yes. Proposed 10 USC 4664(a)(3) has the contractor providing the right to diagnose, maintain, and repair the covered defense equipment.	Yes. Proposed 10 USC 4664(d) requires rights consistent with 10 USC 3771.
License for government contractor use of technical data for repairs	Yes. 10 USC 3774 requires the government to enter into a Specifically Negotiated License Rights (under DFARS 252.227-7013) with the contractor to support the product support strategy for a major weapon system and subsystem of a major weapons system.	Yes. Proposed 10 USC 4664(d) has the contractor not imposing restrictions on authorized maintenance providers for use of ICOR.	Yes. Proposed 10 USC 4664(d) requires contractors to provide the right to the authorized contractor consistent with 10 USC 3771.

Introduction

Recently, there has been a growing public policy discourse about where IP and data rights fit into readiness and sustainment. The so-called “Right to Repair” initiative, championed by some in government, will not solve the issues it seeks to address and will largely result in a withdrawal of innovative companies willing to work with the DoD. RTR disincentivizes research and development (R&D) investment, weakens government-industry partnership models, undermines trade secrets and proprietary design protections, and could even expand to reverse engineering and reproduction. Moving forward, it is imperative to understand the varying use cases that government and industry are working to address and where alternative solutions related to IP can harness private sector innovations to bolster readiness.

Over the past decade, the legal and regulatory framework governing intellectual property rights and the management of these rights has undergone careful reform to balance the legitimate needs of both the Department of Defense (DoD) and industry.⁴ The importance of this balance is evident in the core principles of DoD’s IP policy, which directs the Department to “negotiate specialized provisions when it better aligns DoD and industry interests” and to “respect and protect IP resulting from technology development investments.”⁵

Protecting IP rights not only fosters innovation and attracts new suppliers and private investment to the U.S. defense industrial base (DIB) but also ensures the military has continued access to crucial information and technical data needed to support military equipment throughout its lifecycle. The current approach also drives down costs

to the government as contractors are not required to account for the full value of their IP rights in their proposed price for every contract, ensuring the government is only paying for what it needs. **In essence, respecting and protecting the private sector’s IP rights safeguards the Department’s own long-term interests.**

Some issues that are incorrectly flagged as IP problems uncover other organizational processes and contracting issues that have failed. Other issues arise over misunderstanding the difference between IP, data rights, and technical data, which all refer to very different things in the Defense Federal Acquisition Regulation Supplement (DFARS), but are used by some interchangeably. This drives miscommunication between government and industry, resulting in the underutilization of DoD’s current authorities and leading to a failure to license the correct IP and ensure the IP maps to deliverables in sustainment.

Current NDA A Right to Repair Proposals

The current debate around DoD’s RTR garnered attention in 2024 with Section 828 of the Committee-passed Senate version of the FY2025 NDA A.⁶ At the time, 63 industry associations—representing a diverse coalition of IP stakeholders—expressed concern with the language,⁷ and the amendment was ultimately not adopted. Currently, there are two similar pending proposals under consideration in the FY2026 NDA A.

Senate NDAA Right to Repair

Section 836 of the Senate Armed Services Committee-passed FY2026 NDAA proposes a new concept called "instructions for continued operational readiness (ICOR)" and to make ICOR a mandatory requirement of all future DoD contracts.⁸ ICOR includes data, tools, and software for operations, maintenance, installation, and training, which could include sensitive and proprietary technical and manufacturing data and IP developed at the contractor's private expense. Under this proposal, DoD would be allowed to provide these parts, tools, and information to any authorized third-party contractor, including direct competitors. If the DoD assesses that a contractor is not complying, the Department may withhold payment, enforce contract penalties, reduce performance ratings, or exclude the contractor from future contracts.⁹

The provision also unilaterally authorizes "alternative maintenance or repair actions" for equipment, which includes reverse engineering and fabrication of parts by the DoD or third parties, if it believes the contractor is failing to comply or under wartime conditions. While DoD is required to give the contractor 30 days to comply, there is no appeals process. In addition, even if the contractor is complying, DoD would still be allowed to pursue such alternative maintenance or repair actions if it would "result in significant cost savings." Finally, the provision allows DoD to waive these contract requirements "if the product support strategy and associated business case analysis for the covered defense equipment indicates that the Government does not have a justified need for ICOR."¹⁰

House NDAA Right to Repair

The House Armed Services Committee-passed version of the FY2026 NDAA also includes a modified version of an RTR proposal that applies to major weapons systems.¹¹ Similar to other proposals,¹² the provision mandates that contractors agree to allow DoD "fair and reasonable" access to all repair tools and information, including sensitive IP, which the DoD can then provide to third parties, including competitors. The Original Equipment Manufacturer (OEM) must offer the repair materials at a price that is equivalent to or better than the most favorable prices, terms, and conditions offered to a reseller or distributor. If the OEM does not currently offer the repair material to another provider, the provision mandates that the OEM still has to provide this information at a price considered by the government to be "fair and reasonable." The provision also mandates that the OEM must provide the government with sensitive, proprietary IP developed solely at private expense for a "fair and reasonable licensing fee."¹³

Reducing Innovation and Industry Concerns with RTR Proposals

Generally, respecting the private sector's IP rights and more closely aligning with commercial practices enables the DoD to incentivize investment, which provides the Department with greater access to the most advanced technological innovations. However, the various RTR

proposals will hamper innovation and DoD's access to cutting-edge technologies by deterring companies, including traditional contractors, nontraditionals, and small businesses, from contracting with the DoD over concerns of forcing disclosure of IP; increasing legal, safety, and compliance risks; and introducing contractual and licensing conflicts.

Reducing Access to Innovation

When a company develops new technology, it has potential future value, not only for the Department but also for the commercial market. If a business fears it may lose its IP, which could potentially be the "crown jewel" underpinning the entire business, the company may simply choose not to contract with DoD and protect its future value on the commercial market. If a business elects to contract with DoD, accepting the risk of losing its IP rights, the company would account for that risk in its proposed price, which would limit the government's ability to maximize value. Alternatively, the company may decide to develop two different versions of a product: one for the government and one for the commercial sector. This could result in a better product going into a commercial offering or to another commercial entity that may or may not be willing to sell to the government, depending on outside investor decisions.

In NDIA's *Vital Signs 2025 Survey*, 37% of private sector respondents said their company decided not to include certain technologies in bids because of IP concerns, which is an increase of nine percentage points over the 2024 survey.¹⁴ In addition, over one-third (36%) of private sector respondents chose not to bid on certain DoD contracts out of fear that DoD requirements for IP would put their company's rights at risk, which is an increase of 14 percentage points over last year's survey.¹⁵ This data shows that even before RTR mandates, more companies are already choosing not to contract with the DoD over fear of losing their IP. RTR mandates will further discourage companies from contracting with the DoD and investing in R&D focused on defense applications, which ultimately limits DoD's access to the most innovative and cutting-edge technologies.

Forcing Disclosure of Sensitive Proprietary IP

RTR proposals mandate that contractors provide repair materials, which can include proprietary software tools, technical data, specialized manufacturing techniques, and other trade secrets as a condition of contracting with the DoD. This also includes proprietary IP completely developed by private expense without government funding. The DoD is then able to share this sensitive information with various third parties, which can include an OEM's direct competitors.

In addition to increasing the risk of U.S. innovations falling into the hands of our adversaries through unauthorized dissemination of sensitive information, forcing IP disclosure also weakens long-standing IP protections by exposing U.S. company innovations to reverse engineering and IP misappropriation, both domestically and internationally. This loss of IP creates a competitive disadvantage for U.S. companies, allowing competitors, third-party providers, and potentially international companies to replicate and/or misuse sensitive proprietary technologies. This type of IP loss further deters companies from contracting with the DoD.

Increasing Legal, Safety, Compliance, and Contractual Risks and Conflicts

Although there is an attempt to define “fair and reasonable” within the RTR proposals, the unilateral control given to the government to define the prices, terms, and conditions surrounding a company’s IP and associated repair materials introduces risk and legal ambiguity, which creates a further chilling effect on participation in DoD contracts. For example, contractors may face compliance risks related to prior licensing and sales agreements, including with exports, since each of these may have terms that could be arguably more favorable when viewed in isolation. Additionally, defense systems often integrate third-party IP under restrictive licenses, and OEMs may be unable to legally share certain tools and information without violating those agreements under the proposed RTR mandates. This would force companies to forgo contracting with the DoD to avoid breach of contract or False Claims Act risk, which again will limit DoD’s access to innovation.

In addition, the proposed RTR mandates introduce a level of potential safety risk. While utilizing additive manufacturing to 3D-print a door handle or a small hatch may introduce little risk, many components on advanced platforms can fail without being produced under the most favorable conditions with properly trained technicians. As an example, manufacturing an aileron¹⁶ for a military aircraft outside of an extremely controlled environment with highly trained personnel would simply introduce too great a risk to the performance of the aircraft and the safety of the pilot. Many advanced components are manufactured utilizing specific materials with advanced techniques in exacting environments to extremely precise standards.

Existing and Alternative Solutions

It is imperative to identify the root cause of the specific issues and where IP may or may not be impacting readiness. As it relates to IP, policymakers should consider the specific use cases they are trying to solve, as different scenarios require different solutions. For example, one type of use case is a 30-year-old platform with parts the OEM no longer produces, and DoD is unsure of whether there are other repair materials options. This would require one approach. A second type of use case involves a newer system where the DoD did not initially negotiate and contract for data rights the Department now realizes it needs for long-term sustainment. This would require a different approach.

There are likely other use cases where it would be necessary, perhaps through an established joint industry-government panel, to thoroughly review the current repair authorization processes, how IP and data rights interact with these processes, and what policy changes are needed to solve for specific use cases. **As an initial step, the DoD and Military Services should work toward ensuring that contracting officers and IP contracting specialists are adequately trained and staffed to fully utilize the current authorities related to contracting for the technical data rights and software needed for sustainment.**

Current DoD Authorities Available for Data Rights and IP

There are more creative and surgical solutions being proposed that would have a more positive impact than the RTR proposals. But DoD does not need to wait to start fully leveraging the current authorities it already has for data rights and IP.

For example, in situations where the government determines that it requires a specific repair capability in a specific component, Congress has provided DoD with several authorities and choices that can be used to obtain repair capabilities. Current DoD practice already routinely acquires from its contractors the technical data needed for operations and maintenance of its weapons systems. By way of example, a review of the publications available through the Army Publications Directorate includes over 6,700 technical manuals that the warfighter can use to maintain and operate their equipment.¹⁷ These are ordered under regulations implementing 10 USC 3772,¹⁸ with regulations requiring specific licenses for technical data necessary for operations and maintenance included in 10 USC 3771.¹⁹ In addition, where the government lacks a repair capability even with the current practice, as detailed below, there are additional authorities which the government can use to obtain the capability, which emphasize flexibility and negotiation to allow for different business models (including commercial and nontraditional companies).

Access to Repair Instructions

The government’s ability to use a repair instruction hinges on its having contracted to acquire them from the relevant OEM. The government has existing processes for identifying and ordering technical data under 10 USC 3772.²⁰ Additionally, Congress has legislated a requirement to ensure that the warfighter’s needs are met in 10 USC 4236.²¹ **Under 10 USC 4236, the government is required to negotiate “a price for technical data to be delivered under a contract for such development, production, or sustainment.”** The requirement to negotiate is expressly prior to “selecting a contractor for the engineering and manufacturing development of a major weapon system, production of a major weapon system, or sustainment of a major weapon system.”²² Directly speaking, the requirement to obtain the technical data packages needed to effectuate a repair capability is already a statutory requirement, and this requirement is to be satisfied prior to entering into a contract.

When the repair is not one that can be done in the field, a public-private partnership under 10 USC 2474²³ provides another way to access repair instructions. This authority allows the contractor to set up a supply chain relationship with the appropriate Center of Industrial and Technical Excellence (contract, subcontract, or otherwise) and to use the Center to perform the repair work for the government. Since the contractor has a prime contract that requires the contractor to perform repairs, this subcontract incentivizes the contractor to provide access to the repair instructions needed to perform the repair and

creates a second source for authorized repairs. Additionally, since the depot is a subcontractor performing repairs for the contractor, the contractor is incentivized to provide training and tooling to ensure the depot is able to perform the repairs. Like other transaction authorities, the public-private partnership arrangement is not governed by the Federal Acquisition Regulation (FAR) or DFARS and allows maximum flexibility, but is limited to the Center under the subcontract.

Additionally, there are practical steps that the government can take under the current system to ensure that it has the necessary right to repair. The best place to resolve these issues is pre-award, where competitive market forces drive the best outcomes for the parties. For example, the government can structure a competition to evaluate an offeror's proposed approach to the right to repair as part of a best-value award decision. Offerors would then be motivated to include affordable and practical solutions for the government's right to repair, while the government would be able to engage in discussions as needed to make informed tradeoffs and reach a fair result. The government could include an attachment to the solicitation that identifies its right-to-repair objectives, along with associated Contract Data Requirements List delivery requirements and pricing instructions. This would require the contractor to deliver Specifically Negotiated License Rights that align with the government's right to repair objectives, with the technical data necessary to repair the product at a fair and reasonable price. This approach aligns with best practices from the commercial marketplace and encourages companies to collaborate with DoD to provide innovative technologies.

Rights to Use Repair Instructions

Policymakers are also examining situations in which repair instructions are delivered to the government but are restricted due to privately developed or commercial processes. Under these circumstances, the contractor is entitled to apply a Limited Rights or Commercial Rights restriction on the government's ability to provide the repair instructions to third parties or use the repair instructions to manufacture a spare.

A central point of contention in the policy debates is when DoD requires contractor depot artisans. In these circumstances, the government has historically demanded overly broad licenses, such as Unlimited Rights or Government Purpose Rights, that well exceed a specific use. Contractors are often concerned about providing their repair instructions if the government is licensed to provide them to all possible contractors, including competitors, as in the case of Unlimited Rights or Government Purpose Rights. However, contractors are more likely to provide more limited rights, which support the use of contractor depot artisans.

Congress has provided two different authorities to incorporate contractor depot artisans into their organic depot capabilities. The first authority is the preference for Specifically Negotiated Licenses under 10 USC 3774.²⁴ Under this preference, the government, "to the maximum extent practicable," shall "negotiate and enter into a contract with a contractor for a specially negotiated license for technical data to support the product support strategy of a major weapon system or subsystem of a major weapon system." This preference is a mechanism to "acquire [from contractors] customized technical data

appropriate for the particular elements of the product support strategy."²⁵ This requirement supports the requirement of 10 USC 4236 by providing contractors with a fourth option, which can be customized to meet the needs of both the warfighter and the contractor.

The second authority is the license that is included in the subcontract under a public-private partnership under 10 USC 2474. As noted above, this authority allows the contractor to set up a supply chain relationship with the appropriate Center of Industrial and Technical Excellence. The subcontract is designed for flexibility in how the contractors restrict the usage of repair instructions to those contractor depot artisans needed to support the Center in performing the repairs, in a manner that is not possible under normal FAR and DFARS procurements.²⁶ **This second authority is more consistent with licenses possible under Other Transactions or data-as-a-service (DaaS) subscription agreements.**

Creative and Surgical Solutions for IP and Data Rights

Inventory of Technical Data Rights for Weapons System Sustainment

During the debate over RTR, an alternative solution was offered by Representative Brad Finstad to the FY2026 NDAA.²⁷ The Finstad Amendment would require each Service Acquisition Executive (SAE) to conduct an inventory of technical data and software related to the sustainment of "covered systems," which includes a major defense acquisition program or an acquisition program or project carried out using the rapid fielding or rapid prototyping acquisition pathway.

After completing the inventory, the SAE would then identify the technical data and software that the Executive has taken delivery of, has current access to, or has negotiated terms to enable guaranteed access or delivery at a future date. Finally, the SAE would identify areas where the DoD has insufficient access to technical data and software needed for sustainment and then work with the relevant contractor to identify the best approach to remedy an identified insufficiency in covered data in the most cost-effective manner practicable.

It is important to note, however, that when a servicemember is required to perform the repair or when a government employee at a depot is performing the repair, the existing Limited Rights or Commercial Rights license allows DoD personnel to perform the repair.

The Finstad Amendment approach would help the Department and Military Services identify any deficiencies related to data rights and sustainment and remedy the specific issues while respecting the IP rights of U.S. industry. This would also enable the creation of a centralized repository outlining the data rights and software the DoD and Military Services have access to for their weapons systems, to quickly address issues moving forward.

Data-as-a-Service (DaaS)

Another creative solution was introduced by Chairman Mike Rogers in H.R. 3838, the SPEED Act, and was included in the Chairman's Mark for the FY2026 NDAA.²⁸ Similar to the concept of other cloud-based services, such as Infrastructure-as-a-Service or Software-as-a-Service, Chairman Rogers proposed data-as-a-service (DaaS) for weapons systems. The proposal would enable DoD to contract for technical data or software and only pay for what the Department uses for the performance of depot-level maintenance and repair by employees of DoD or the maintenance of a core logistics capability.

Instead of contracting for all of the data rights the Department believes it will need for all future sustainment for a particular platform up-front, the DaaS model allows the government and OEM to set up a framework where all the necessary technical data or software is accessible, but the Department only pays if and when it utilizes the covered data for a repair or to manufacture a single part. The transfer of the covered data can be made available electronically, in-person, or via machine-to-machine encryption, as appropriate, depending on the type, sensitivity, or authorized use of the information. DaaS allows contractors to include an associated license agreement that provides the government with limited access to the necessary technical data or computer software to repair the weapons system using the most up-to-date information for a reasonable fee and only for the limited time required for the repair.

The DaaS approach is a cost-effective solution for the DoD to ensure access to the technical data and software needed for sustainment while allowing the OEM to maintain control of its sensitive and proprietary IP.

Understanding the Real Challenges of Readiness and IP's Role

DoD has a well-documented maintenance and sustainment problem, which directly impacts the Joint Force's current and future requirements. In fact, of the six "top DoD management and performance challenges" identified by DoD Inspector General (IG), the first on the list was "Increasing Military Readiness,"²⁹ which includes limited availability of functional equipment for executing missions.

In addition, according to the Government Accountability Office (GAO):

- From 2011 through 2021, "sustainment challenges worsened" for 10 Navy ship classes, leading to a decrease in the number of ship availability hours for operations or training.³⁰
- In 2023, the Navy's surface ship maintenance backlog was \$1.8 billion.³¹
- In 2024, DoD did not meet "its mission capable rate goals for fiscal year 2024 for 42 of the 45 DoD aircraft that support military-related missions."³²

The path to improved readiness is having the right infrastructure, effective IT systems, sufficient spare parts, and an effective maintenance workforce. In working to address these challenges, policymakers are also examining whether the government's access to IP is contributing to the readiness challenge. This was reflected in policy debates in 2018 and 2019, which pointed to the lack of access to technical data as one issue.³³ However, subsequent enacted legislation, improved training, and updated policy guidance (including the creation of the IP Cadre) have provided the tools needed to remedy the identified issues. An analysis of recent GAO reports, DoD IG audits, independent analysis, and DoD statements also indicates that IP is not the main issue for readiness.

For example, according to GAO, Navy executive officials identified the lack of spare parts, the lack of trained maintenance personnel, and increases in deferred maintenance as long-running problems that prevented maintenance during deployment, increased the cost of repairs, and reduced ship service life and operational readiness.³⁴ Even if all the IP issues were resolved tomorrow, the operational crisis would still prevent the Navy from taking advantage of the situation.

Other maintenance challenges identified as directly impacting Navy readiness include aging equipment, canceled maintenance, reliability of ship systems, and inefficient shipyard layouts (an infrastructure issue).³⁵ Aging equipment and inadequate maintenance have been identified as DoD-wide challenges.³⁶ IP was not highlighted as the main issue in any of these lists of readiness challenges.

Infrastructure

One of the more severe challenges to improved readiness is infrastructure. Even when the government has the IP with the associated licenses needed to perform the repair, without adequate infrastructure, the government cannot perform the repair. The Navy reported that without improvements to shipyard infrastructure, it will be unable to support almost a third of the planned maintenance periods for aircraft carriers and submarines through 2040. According to GAO, dry docks and maintenance facilities are poor, and equipment is “generally past its useful life.”³⁷ The Army also faces infrastructure challenges. The organic industrial base performs a lot of remanufacturing and maintenance. The average organic industrial base factory is 80 years old.³⁸ Stephanie Hoaglin, the director of the Army’s Organic Base Modernization Task Force, stated that the Army has an \$18 billion, 15-year plan to upgrade infrastructure, improve equipment and processes, and “bring all those things to the 21st century.”³⁹

Effective IT Systems and Data Management

Poor data management—and mismatched computer systems—directly undermine readiness. In one recent example, the Army relies on Defense Logistics Agency (DLA) for 90% of its maintenance parts—mostly low-dollar, high-volume expendables.⁴⁰ Yet, until recently, the Army and DLA operated with incompatible systems, creating supply chain disruptions and hurting readiness. DLA was unable to assess what supplies the Army was consuming and was unable to order the necessary parts before they were needed, a significant challenge when some parts have a two-year delivery time.⁴¹

In another example, DoD IG’s analysis of spare parts on Navy ships found that the spare parts “inventory accuracy was between 83 and 95 percent, which is below the minimum inventory accuracy of 98 percent needed to ensure the ships’ readiness.”⁴² The inventory discrepancies in the Navy’s RSupply software application (intended to provide real-time, online tools for inventory management) were attributed to:

- Not knowing where the parts were
- Not updating inventory records after issuing spare parts
- Not removing excess line items from the ships

As a result, the IG found that “the Navy did not have assurance that the 10 ships we reviewed in the Indo-Pacific region had all of the required spare parts...to maintain operational readiness.”

These are not IP problems; they are IT problems. However, IT and data management are also key drivers to DoD’s IP challenges. DoD has the legal authorities and updated policy guidance (including the creation of the IP Cadre) it needs to effectively negotiate for, manage, and use, data rights and IP. What DoD lacks is a systematic method to keep track of IP rights across the Military Services and even between programs, leading to wasteful and duplicative licensing of the same technology by different programs. The IP problem, however, is driven in part by ineffective IT systems and data management.

Workforce

The Navy has stated that it lacks sufficient trained maintenance personnel to maintain combat surface ships.⁴³ In addition, DoD personnel, including maintainers, are overworked and understaffed.⁴⁴ DoD’s workforce is not sufficiently experienced in how to contract for IP and data rights licenses for sustainment and maintenance, which is another indication of where DoD’s actual IP challenges manifest in other areas.

Effectively Building Readiness

DoD and Congress could take steps to substantially improve readiness. For example, GAO has highlighted the need for DoD to further implement predictive maintenance, which would increase operational availability of weapon systems.⁴⁵ Other opportunities to improve readiness include:

- Modernizing IT systems to ensure data reliability and interoperability
- More widely implementing predictive maintenance
- Investing in modern, efficient maintenance facilities and equipment
- Ensuring a right-sized, properly trained workforce, and well-managed
- Not deferring needed maintenance

DoD is also not effectively using the tools it already has to manage and access data rights and IP. DoD needs to do a better job of including detailed IP Asset Schedules, mapped onto deliverables and sustainment use cases in contracts. Product support managers should be more involved in IP budget formation early in the procurement process. The DoD also needs to do a better job of communicating the use cases for data rights to industry.

Only by more effectively using the authorities it already has, implementing good contracting practices, and addressing the core issues outlined above, will DoD improve operational readiness.

Closing

Ultimately, the most effective way for DoD to maximize access to IP for sustainment is to ensure the Department is a fair, collaborative partner with industry in the shared mission to provide U.S. service-members with the most advanced, best-maintained equipment possible. Pursuing RTR will further deter more innovative companies from working with the Department to the detriment of DoD’s access to the most cutting-edge technologies, which is a trend we are already seeing related to the fear of losing IP. The more companies seek to work with DoD, the more access the Department will have to capabilities that are innovative, cutting-edge, and driven by IP.

Endnotes

- 1 National Defense Industrial Association. Vital Signs 2025. February 26, 2025. www.ndia.org/vitalsigns.
- 2 U.S. House of Representatives, 119th Congress, 1st Session, Armed Services Committee. Reforming Defense Acquisition to Deliver Capability at the Speed of Relevance. July 23, 2025.
- 3 U.S. Representative Brad Finstad. Amendment to H.R. 3838. Log 5633, Revision 1. Chairman's Mark En Bloc #5. July 15, 2025. https://armedservices.house.gov/uploadedfiles/chm_en_bloc_5.pdf.
- 4 P.L. 114-328. Section 809; P.L. 115-91. Section 802.
- 5 U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition and Sustainment. DoD Instruction 5010.44. Intellectual Property (IP) Acquisition and Licensing. October 16, 2019. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/501044p.pdf>.
- 6 U.S. Senate, 118th Congress, 2nd Session. S.4368 – National Defense Authorization Act for Fiscal Year 2025. Placed on Senate Legislative Calendar under General Orders. Calendar No. 433. July 8, 2024.
- 7 National Association of Manufacturers. Industry letter to Representatives Jack Reed and Mike Rogers and Senators Roger Wicker and Adam Smith. July 30, 2024. <https://documents.nam.org/LLRP/Signed.FY25.NDAA.Section.828.Letter.pdf>.
- 8 U.S. Senate, 119th Congress, 1st Session. S.2296 - National Defense Authorization Act for Fiscal Year 2026. Placed on Senate Legislative Calendar under General Orders. Calendar No. 115. July 15, 2025.
- 9 Ibid.
- 10 Ibid.
- 11 U.S. House of Representatives, 119th Congress, 1st Session. H.R.3838 – Streamlining Procurement for Effective Execution and Delivery and National Defense Authorization Act for Fiscal Year 2026. Ordered to be Reported (Amended) by the Yeas and Nays: 55 - 2. July 15, 2025.
- 12 U.S. Senator Elizabeth Warren. S.2209 – Warrior Right to Repair Act of 2025. Introduced July 8, 2025.
- 13 U.S. House of Representatives, 119th Congress, 1st Session. H.R.3838 – Streamlining Procurement for Effective Execution and Delivery and National Defense Authorization Act for Fiscal Year 2026. Ordered to be Reported (Amended) by the Yeas and Nays: 55 - 2. July 15, 2025.
- 14 National Defense Industrial Association. Vital Signs 2025. February 26, 2025. www.ndia.org/vitalsigns. Page 29.
- 15 Ibid
- 16 An aileron is a hinged flight control surface, typically found on the trailing edge of an aircraft's wings, used to control the aircraft's roll movement.
- 17 Army Publishing Directorate. Latest Administrative Publishing Actions. Accessed August 8, 2025. <https://armypubs.army.mil/default.aspx>.
- 18 10 USC 3772: Rights in technical data: provisions required in contracts. Text contains those laws in effect on August 5, 2025.
- 19 10 USC 3771; Rights in technical data: regulations. Text contains those laws in effect on August 5, 2025.
- 20 10 USC 3772: Rights in technical data: provisions required in contracts. Text contains those laws in effect on August 5, 2025.
- 21 10 USC 4236: Negotiation of price for technical data before development, production, or sustainment of major weapon systems. Text contains those laws in effect on August 5, 2025.
- 22 Ibid.
- 23 10 USC 2474: Centers of Industrial and Technical Excellence: designation; public-private partnerships. Text contains those laws in effect on August 5, 2025.
- 24 10 USC 3774: Major weapon systems and subsystems: long-term technical data needs. Text contains those laws in effect on August 5, 2025.
- 25 Ibid.
- 26 10 USC 2474: Centers of Industrial and Technical Excellence: designation; public-private partnerships. Text contains those laws in effect on August 5, 2025.
- 27 U.S. Representative Brad Finstad. Amendment to H.R. 3838. Log 5633, Revision 1. Chairman's Mark En Bloc #5. July 15, 2025. https://armedservices.house.gov/uploadedfiles/chm_en_bloc_5.pdf.
- 28 Representative Mike Rogers. H.R.3838 – Streamlining Procurement for Effective Execution and Delivery and National Defense Authorization Act for Fiscal Year 2026. Ordered to be Reported (Amended) by the Yeas and Nays: 55 - 2. July 15, 2025.
- 29 U.S. Department of Defense, Inspector General. Top DoD Management and Performance Challenges Fiscal Year 2025. October 15, 2024. https://media.defense.gov/2024/Nov/15/2003584454/-1/-1/1/MANAGEMENT%20CHALLENGES%20FY2025_SIGNED_15NOV.PDF. Page 11.
- 30 U.S. Government Accountability Office. Weapon System Sustainment: Navy Ship Usage Has Decreased as Challenges and Costs Have Increased. GAO-23-106440. January 31, 2023. <https://www.gao.gov/products/gao-23-106440>.
- 31 U.S. Government Accountability Office. Military Readiness: Improvement in Some Areas, but Sustainment and Other Challenges Persist. GAO-23-106673. May 2, 2023. <https://www.gao.gov/assets/gao-23-106673.pdf>. Page 19.
- 32 U.S. Government Accountability Office. Military Readiness: Implementing GAO's Recommendations Can Help DoD Address Persistent Challenges across Air, Sea, Ground, and Space Domains. GAO-25-108104. March 12, 2025. <https://www.gao.gov/assets/gao-25-108104.pdf>. Page 17.
- 33 813 Panel. 2018 REPORT GOVERNMENT-INDUSTRY ADVISORY PANEL ON TECHNICAL DATA RIGHTS. NOVEMBER 13, 2018. www.dau.edu/sites/default/files/Migrated/CopDocuments/Section%20813%20Report.pdf. Van Atta, Richard, et al. "Department of Defense Access to Intellectual Property for Weapon Systems Sustainment." Institute for Defense Analysis. May 2017. <https://www.ida.org/research-and-publications/publications/all/d/de/departament-of-defense-access-to-intellectual-property-for-weapon-systems-sustainment>. The Department committed to implementing the recommendation of both reports in its letter to Congress on February 3, 2019, sent by Under Secretary of Defense (Acquisition and Sustainment) Ellen Lord.
- 34 U.S. Government Accountability Office. Navy Surface Ships: Maintenance Funds and Actions Needed to Address Ongoing Challenges. GAO-25-106990. January 31, 2025. <https://www.gao.gov/products/gao-25-106990>.
- 35 U.S. Government Accountability Office. Navy Readiness: Actions Needed to Address Cost and Schedule Estimates for Shipyard Improvement. GAO-23-106067. June 28, 2023. <https://www.gao.gov/products/gao-23-106067>; U.S. Government Accountability Office. Amphibious Warfare Fleet: Navy Needs to Complete Key Efforts to Better Ensure Ships Are Available for Marines. GAO-25-106728. December 3, 2024. <https://files.gao.gov/reports/GAO-25-106728/index.html>.
- 36 U.S. Department of Defense, Inspector General. Fiscal Year 2025 Top DoD Management and Performance Challenges. November 15, 2024. https://media.defense.gov/2024/Nov/15/2003584454/-1/-1/1/MANAGEMENT%20CHALLENGES%20FY2025_SIGNED_15NOV.PDF.

IP and Data Rights: Protecting DoD's Access to Innovation

- 37 U.S. Government Accountability Office. Navy Readiness: Actions Needed to Address Cost and Schedule Estimates for Shipyard Improvement. GAO-23-106067. June 28, 2023. <https://www.gao.gov/products/gao-23-106067>.
- 38 Temin, Tom. "How the Army goes about modernizing its crucial but aging organic industrial base." Federal News Network. October 17, 2024. <https://federalnewsnetwork.com/army/2024/10/how-the-army-goes-about-modernizing-its-crucial-but-aging-organic-industrial-base/>.
- 39 Ibid.
- 40 Richard Martin, Army Materiel Command's Director for Supply Chain Management, quoted in: Williams, Lauren C. "Is bad data to blame for missing weapons parts?" Defense One. January 17, 2025. <https://www.defenseone.com/defense-systems/2025/01/bad-data-blame-missing-weapons-parts/402324/>.
- 41 Ibid.
- 42 U.S. Department of Defense, Inspector General. Evaluation of the Spare Parts Onboard U.S. Navy Ships in the Indo-Pacific Region. Report No. DODIG-2025-100. May 14, 2025. https://media.defense.gov/2025/May/15/2003715601/-1/-1/1/DODIG-2025-100_REDACTED_FINAL_SECURE.PDF.
- 43 U.S. Government Accountability Office. Navy Surface Ships: Maintenance Funds and Actions Needed to Address Ongoing Challenges. GAO-25-106990. January 31, 2025. <https://www.gao.gov/assets/gao-25-106990.pdf>. Page 9.
- 44 U.S. Government Accountability Office. Military Readiness: Comprehensive Approach Needed to Address Service Member Fatigue and Manage Related Efforts. GAO-24-105917. March 26, 2024. <https://www.gao.gov/assets/gao-24-105917.pdf>; Campbell, Austin. "Decades of Troubles for Air Force Maintainers Set to Get Worse with Job Consolidation." Military.com. July 25, 2025. https://www.military.com/daily-news/investigations-and-features/2025/07/25/decades-of-troubles-air-force-maintainers-set-get-worse-job-consolidation.html?utm_campaign=dfn-ebb&utm_medium=email&utm_source=sailthru.
- 45 U.S. Government Accountability Office. Military Readiness: Actions Needed to Further Implement Predictive Maintenance on Weapon Systems. GAO-23-105556. Dec. 8, 2022. <https://www.gao.gov/products/gao-23-105556>.

NDIA

The National Defense Industrial Association is the trusted leader in defense and national security associations. As a 501(c)(3) corporate and individual membership association, NDIA engages thoughtful and innovative leaders to exchange ideas, information, and capabilities that lead to the development of the best policies, practices, products, and technologies to ensure the safety and security of our nation. NDIA's membership embodies the full spectrum of corporate, government, academic, and individual stakeholders who form a vigorous, responsive, and collaborative community in support of defense and national security. For more than 100 years, NDIA and its predecessor organizations have been at the heart of the mission by dedicating their time, expertise, and energy to ensuring our warfighters have the best training, equipment, and support. For more information, visit [NDIA.org](https://www.ndia.org)