VARONIS

DISA Data Strategy Implementation Plan

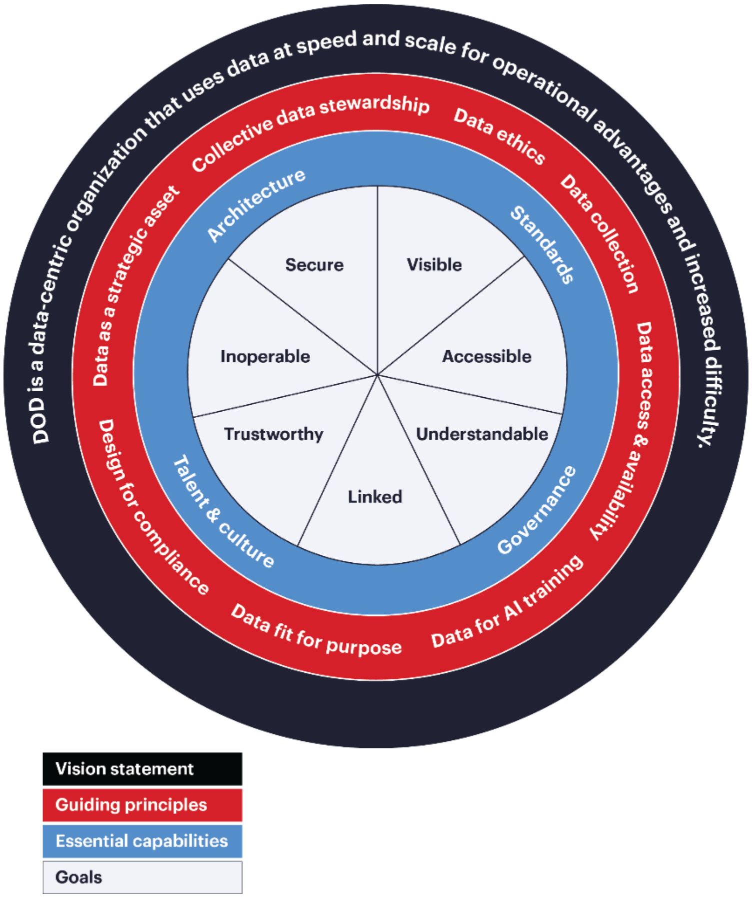
Mapping Varonis offerings
to the DISA Data Strategy IPlan

Contents

The objective of the DISA Data Strategy Implementation Plan (IPlan)

The primary role of the Defense Information Systems Agency (DISA) is to support U.S. Department of Defense (DOD) operations with IT and communications. Recently, DISA initiated the process of a strategic transformation effort to “improve the state of its data, information technology (IT), and network capabilities to better support the DISA mission, gain efficiencies, and lower support costs” (DISA Data Strategy IPlan v1.0).[1]

The DISA Data Strategy Implementation Plan (IPlan) is a key component of this transformation. The IPlan follows the guiding principles of the recently published DOD Data Strategy, and as such, proposes five strategy areas, named “lines of effort,” for fulfilling the requirements for architecture, standards, talent and culture, and governance. The IPlan adopts the same principles as the DOD Data Strategy, as well as their own supplemental guidelines, with the goal of ensuring data is **VAULTIS**:



Visible — Data consumers can locate mission-critical data.

Accessible — Consumers can retrieve this data without difficulty.

Understood — Consumers can recognize the content, context, and applicability of mission data.

Linked — Consumers can exploit data elements through innate relationships.

Trusted — Consumers can be confident in all aspects of data for decision-making.

Interoperable — Consumers have a common representation/ comprehension of data.

Secure — Data stewards know that data is protected from unauthorized use, access, and manipulation.

Data-centric security

The Varonis Data Security Platform is uniquely positioned for this data-centric approach to improving the state of DISA's IT and network capabilities.

Knowing where you have sensitive data and who can access it is a critical first step in ensuring data security. Once you have visibility into where sensitive data lives across different data stores, you need to understand who can access it and what they're doing with it to be able to identify where that data may be overexposed and when it might be compromised.

From a practical perspective, keeping data safe is impossible without automation. Automation ensures we can handle the scale at which data grows and the complexity of how that data should be handled. From a data security perspective, automation is a necessary approach for remediation.

Lastly, you need continuous monitoring and alerting to detect cyberattacks and a plan to respond to these attacks within the required timeframe (should they occur).

Mapping Varonis to the DISA Data Strategy IPlan lines of effort

The IPlan outlines four specific lines of effort (LOE) to achieve this goal. Within each LOE are various initiatives with their own respective goals aligning to the overarching strategy. The Varonis platform capabilities map to many of these initiatives spanning all four of the efforts.

Here's how Varonis can help organizations achieve data security as expected by the DISA Data Strategy IPlan:

DISA Data Strategy checklist	How Varonis helps
Data architecture and governance	
Mapped initiatives: • Establish a DISA metadata standard to guide the collection and registration of the essential architecture metadata (LOE 1, Initiative 1). • Identify/catalog/document the agency's data repositories, structures, and attributes; prepare to align to the Chief Data Officer's (CDO) forthcoming data-centric design (LOE 1, Initiative 4).	• Varonis identifies, classifies, and tags your agency's data at petabyte scale. • The platform reports on access and permissions, as well as automates the remediation of overexposure and risk. • Our platform can produce artifacts of current risk management framework (RMF) controls and assist with understanding key metadata for proposing new controls specific to data.

• Create data governance policies for an enterprise approach in order to evolve DISA's data use (LOE 1, Initiative 5). • Complete the required research and analysis to develop a proposal for incorporating data management controls into the risk management framework (RMF) (LOE 1, Initiative 7). • Establish a robust data stewardship framework	• Varonis can identify and assign data owners/stewards to govern the organizational data with easy-to-use workflows. This ensures that business owners can manage their data instead of IT and can “ensure DISA’s data assets are fully employed and intelligently positioned to achieve mission priorities in a nimble and response manner” (Section 4.1.2).
Advanced analytics	
Mapped initiatives: • Evolve data collection, aggregation, and modeling to provide relevant, discoverable, understandable, and trusted information and to enable rapid and effective decision-making within the DOD. Certify that the data infrastructure enables this to be done effectively and efficiently (LOE 2, Initiative 1). • Establish a framework of standards and processes that facilitate the identification, collection, cataloging, and use of the data, both internal to DISA's mission objectives as well as enabling use by our mission partners (LOE 2, Initiative 2). • Establish the framework that enables the agency to analyze and prioritize use cases for DISA data that support the key areas of command and control, senior leader decision support, cybersecurity analytics, and business/mission analysis (LOE 2, Initiative 3). • Enforce metadata tagging standards for data normalization (LOE 2, Initiative 5).	• Varonis is the leading platform in data classification, and catalogs the location, permissions, and access to sensitive data across the agency. Varonis classifies and tags data such as personally identifiable information (PII), personal health information (PHI), controlled unclassified information (CUI), secret and top-secret information, and sensitive government forms, among many more categories. • Our robust classification is enhanced by our ability to label files with a metadata field that perpetuates across your network. This can help you track and enforce organizational policy, reducing the risk of data spillage and enabling end-to-end data governance. • The Varonis threat modeling and alert modules use out-of-the-box user behavior analytics to provide insight into how your data is being used from the day of installation. After installation, Varonis continuously learns what is “normal” for your network to produce fine-tuned alerts and reduce the false positive rate.

Data culture

Mapped initiatives:

- Develop and implement agency-wide training programs to increase general knowledge of data management practices across the workforce and possibly tie training to job function. Offer certifications to the workforce as part of DISA’s ongoing recruitment and retention efforts for job roles focusing on data. Upon completion of the DISA Data IPlan, the CDO office will coordinate best practices to offer training with Workforce Services Directorate (WSD). Integrate all new training content to existing methods of training/certifications (LOE 3, Initiative 1).

- Risk on data often begins when the decisions on access to mission-critical data is outside the hands of those who know their data best: data stewards and owners. Varonis can help your organization with data governance by identifying and assigning data owners across the agency. From an easy-to-use web interface, these data owners can create workflows for ensuring a least-privilege model where only the right users have access to the data.
- Varonis facilitates a data-centric culture across the entire organization by giving the deciding vote of who has access to data over to those that know best, ensuring they are knowledgeable and data-aware.

Knowledge management

Mapped initiatives:

- Knowledge Management Assessment (LOE 4, Initiative 1).
- Expand the agency's knowledge management maturity through the development of fit-for-purpose knowledge portals, dashboards, and content management solutions leveraging existing agency platforms and enablers (LOE 4, Initiative 3).

- Varonis provides dashboards to enable easy periodic assessment of data at risk, effectively providing “performance data and metrics needed to apply refinement actions” (Section 4.4.1).
- Many of our out-of-the-box and custom reports provide all parties involved in knowledge management with unique and correlative data insights. Our alerts and reporting APIs — coupled with native integrations to ITSM, SIEM, and other tools — can assist you in building knowledge management portals, dashboards, and more.

Conclusion

Varonis has partnered with the DOD for years to help commands accomplish their mission objectives surrounding their data. Making the data visible, accessible, understandable, linked, trustworthy, interoperable, and secure can only be done efficiently and successfully when agencies are monitoring the data itself and taking a data-first approach to data management and governance.

Varonis provides essential context to your data by determining its sensitivity, surfacing risks to your data, and providing AI-driven user behavioral analytics with insight into the users and devices accessing agency data. With Varonis, it is possible to begin treating data as a “strategic asset that must be operationalized,” ensuring the data is VAULTIS.[2] Our data-first approach enables the agency to own its data and ensure organizations are not “losing their strategic ability to deploy and exploit data effectively in the battlespace for digital dominance” (Section 4.1.2). Varonis provides a strong foundation to accelerate and efficiently execute the IPlan.

Footnotes:

1. United States Department of Defense. 2020. “DOD Data Strategy: Unleashing Data to Advance the National Defense Strategy.” https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF
2. Office of the Chief Data Officer of the Defense Information Systems Agency. 2022. “DISA Data Strategy Implementation Plan.” https://www.disa.mil/-/media/Files/DISA/News/DISA-Data-Strategy-IPlan-Final-072022.ashx

VARONIS

Schedule a free Data Risk Assessment.

Varonis can help manage your security risk and comply with the DISA Data Strategy IPlan by identifying where you have sensitive data, reducing that data's blast radius, and monitoring that data for potential threats. To see where you have sensitive data across your environment, sign up for a free data risk assessment.

Our complimentary assessment run by expert forensics and incident response analysts based in the United States will help you find and classify regulated data across on-premises and cloud data stores, measure data exposure, and alert on suspicious access to regulated information.

Contact us

About Varonis

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data on premises and in the cloud: sensitive files and emails; confidential customer, patient, and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects insider threats and cyberattacks by analyzing data, account activity, and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation. With a focus on data security, Varonis serves a variety of use cases including governance, compliance, classification, and threat analytics. Varonis started operations in 2005 and has thousands of customers worldwide — comprised of industry leaders in many sectors including technology, consumer, retail, financial services, healthcare, manufacturing, energy, media, and education.