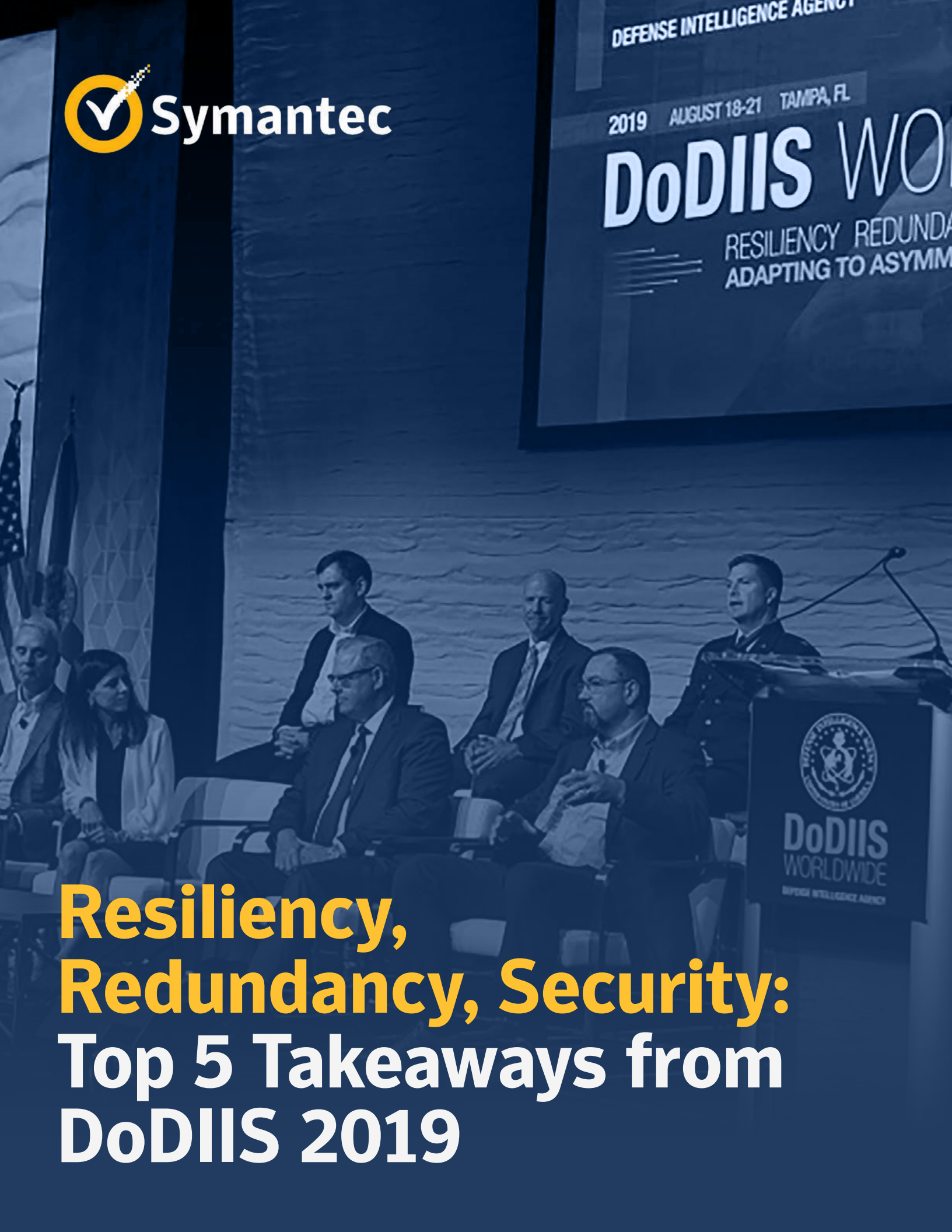


# Resiliency, Redundancy, Security: Top 5 Takeaways from DoDIIS 2019

The Defense Intelligence Agency (DIA) hosted its annual Department of Defense Intelligence Information System (DoDIIS) Worldwide Conference last month. A main focus this year was how to secure defense systems and networks in a world where the sophistication of cyber threats is outpacing the sophistication of cybersecurity.

To successfully carry out their missions, DoD must be able to collaborate in a trusted manner and freely leverage data through technology. Unfortunately, this intersection is also the point of greatest vulnerability for defense organizations, and unless these deficiencies are adequately addressed, they will be unable to properly protect their assets and reap the benefits of technology advances.

Over the course of the three-day conference, leaders from across the intelligence community (IC) discussed critical security challenges, and how best to address them. As existing cybersecurity apparatuses are being pushed to their breaking point, how do we respond? Read on to find out.

## 1: Make Cybersecurity Foundational

Traditionally, security has not been thought about until the last step of a process, but several DoDIIS speakers stressed the importance of "shifting left," meaning involving security in the development, build, test, and deployment stages of any product. Securing mission networks and data should not be confined within IT departments, rather, it should be a "whole-of-government" effort.


An advanced cybersecurity posture requires constant evaluation of all people, processes, and technologies within an organization. To get there, organizations must invest time and resources in the fundamentals, such as establishing an identity, credential, and access management strategy, implementing a multi-factor authentication system, and educating everyone within an organization on minimum security requirements and cyber-hygiene best practices.

> **"There's a trend to be captivated by the most stressing, fascinating thing our adversary is doing… but this tends to draw your attention away from what I call 'blocking and tackling'… You can take the same thought of always chasing the shiniest object, but not having your fundamentals down, and that's a real big challenge."**
> **- Mark Andress, Chief Information Officer, National Geospatial Intelligence Agency**

## 2: Protection Must Extend Beyond the Network Perimeter

While still necessary, the traditional approach of authenticating and determining trust for users at the network's edge is no longer sufficient. As more workflows move to the cloud, and an increasing number of endpoints and users require access from various locations, DoD's attack surface continues to expand. Not only has this created more opportunities for attackers, it has also made it harder for security experts to identify good and bad behavior, making it harder for them to know when and how to intervene. DoDIIS speakers discussed how this necessitates a shift from 'trust but verify,' to 'never trust, always verify.'

"We are fighting a losing battle unless we learn to address problems differently," said Jean Schaffer, chief of cyber and enterprise operations at the DIA.

This strategy, commonly referred to as Zero Trust (ZT), is anchored on the principle that organizations need to proactively control all interactions between people, data, and information systems. Rather than allowing all assets within an organization to be open and available, ZT requires continuous authentication and authorization for any asset to be accessible.

> **"We regularly have to contend with ambiguous, incorrect, and fabricated information, so from a data perspective, the haystack never stops growing, and the needle continues to be more subtle and difficult to find."**
> **- John Doyon, Chief Data Officer and Director, Office of Data Strategy and Innovation at the National Counterterrorism Center**

## 3: Reaping the Benefits of ZT

ZT mitigates many of the shortcomings that plague traditional cybersecurity models. Two commonly referenced benefits were greater data protection and enhanced visibility.

- More securely share data: Defense operations increasingly require better information flow between users and devices. By applying ZT authentication and authorization rules, organizations can grant highly specific access with minimal risk exposure of the rest of their networks. These techniques allow organizations to segment, isolate, and control their data, and make it easier for DoD employees, contractors, and allied forces to access and share information.
- Increased visibility: You can't combat what you cannot see or understand. If an organization develops a baseline of 'normal' network activity, it can then configure tools to alert appropriate people when there is any abnormal behavior on the network. Armed with a picture of what is happening in real time, security experts can ask better questions and more intelligently make policy and trust decisions related to network and data traffic.

"It's imperative for all federal agencies to address a new world of cyber threats that can emerge through trusted insiders, IT networks, supply chains or components themselves. With the ever evolving threat landscape, adopting a Zero Trust methodology now can better protect federal systems and data," said Andrew Borene, senior director of Federal for Symantec's National Security Group.

## 4: Don't Forget About People and Process

DIA CIO Jack Gumtow illustrated the importance of people and process with an example about teleconferencing.

The DIA wanted to include its partners in the Five Eyes intelligence alliance – Australia, Canada, New Zealand, and the United Kingdom – on video teleconference calls. A seemingly straightforward and simple goal, yet, it took two years to implement. Gumtow explained: "It wasn't technically difficult to do; it came down to a policy issue: trying to get the right people to break that down and understand why you wrote that policy in 1989 and why it's no longer relevant in 2018."

Likewise, successful implementation of ZT will hinge on DoD's ability to overcome hurdles related to technical policy issues and cultural bias. For example, in order to build access control for specific applications and services – a central pillar of ZT – missions will have to improve their digital management and tracking of user roles across organizations. This will be a significant undertaking that will not only require thoughtful changes to policy, but also a concerted communications effort to secure buy-in from people at all levels of an organization.

During a breakout session on organizational transformation, panelists discussed the complexity of securing buy-in, particularly within the IC. These leaders stressed the need for outspoken and consistent support from agency leadership, targeted messaging, and finally, as moderator Ian Fowlie said, "a level of strategic patience the IC struggles with."

"We have three different generations and we have to figure out how to reach all of them. We have a leader who sends out biweekly emails, holds town halls, and walks around the office to ask people how things are going. In all three mediums, he reaches different audiences," said DIA Chief of Resources Anthony Howell.

# 5: DIA's Moonshot: The Machine-Assisted Analytic Rapid-Repository System

DIA Director Lt. Gen. Robert Ashley was resolute as he described what he believes to be the most significant problem the DIA and the broader IC face going forward: data interoperability. "Large, complex data sets don't talk to one another, and we've got to fix that." In Ashley's view, interoperability – the ability to transfer information between systems and partners and communicate across platforms – is absolutely critical. Without it, he warned, "We will be sub-optimized and we will miss opportunities."

DIA's flagship effort to make intelligence more accessible to more people is called MARS (Machine-Assisted Analytic Rapid-Repository System). MARS is envisioned as a common intelligence repository of all defense intelligence that users can apply different applications to in order to get the information they need. This would free up analysts to tackle harder problems, instead of sifting through multiple databases. "It should not take a war to share this kind of information."

The conversations throughout DoDIIS underscored the importance and centrality of DIA's mission. As the backbone connecting all of the disparate military entities within the IC, the DIA offers vital support that helps them fulfill their respective missions. Lt. General Robert P Ashley reminded attendees that 2.5 quintillion bytes of data are created every day, and a growing portion of it deliberately faked or twisted into disinformation. This reality, he said, makes the DIA's mandate of providing actionable intelligence in a trusted environment even more critical. While the growing number of asymmetric threats certainly presents challenges, it is also fueling a new era of collaboration and innovation between the DoD, private companies, as well as our military allies, to build systems and tools that are more redundant, resilient, and secure.

*Photos by David Richards courtesy of the Defense Intelligence Agency.*