Top Takeaways From DoDIIS 2024

Thank you for downloading this Axonius Federal Systems article. Carahsoft is the master government aggregator and distributor for Axonius Federal Systems' Cybersecurity solutions available via GSA, NJSBA, Educational Software Solutions and Services – OMNIA Partners, Public Sector, and other contract vehicles.

To learn how to take the next step toward acquiring Axonius Federal Systems' solutions, please check out the following resources and information:

For additional resources:
carah.io/AxoniusFederalResources

For upcoming events:
carah.io/AxoniusFederalEvents

For additional Axonius solutions:
carah.io/AxoniusFederalSolutions

For additional Axonius News:
carah.io/AxoniusFederalNews

To set up a meeting:
Axonius@carahsoft.com
703-214-4790

To purchase, check out the contract vehicles available for procurement:
carah.io/AxoniusFederalContracts

For more information, contact Carahsoft or our reseller partners:
Axonius@carahsoft.com | 703-214-4790

GovCIO MEDIA & RESEARCH

SPECIAL RECAP

SPONSORED BY

AXONIUS FEDERAL

5 Takeaways from DoDIIS 2024

Intelligence Community (IC) leaders gathered in Omaha, Nebraska, to discuss the latest in cybersecurity, integrated deterrence and intelligence systems. Get up to speed on artificial intelligence implementation, zero trust strategy and other highlights from the October 2024 Department of Defense Intelligence Information System (DoDIIS) Worldwide Conference.

01
The IC needs to be data-centric to thrive.

Collecting data is integral to intelligence operations. IC Chief Data Officer Lori Wade noted the challenges and strategies for achieving data centricity within the IC, including the importance of well-managed data.

"We talk about data as a strategic asset, but only if it's managed well. Otherwise, it becomes a liability, a liability from external and insider threats," said Wade. "It also becomes a liability from a cost perspective."

02
Zero trust bolsters IC cyber defenses.

> **"The zero-trust journey is one that we've been on for quite a long time. We implemented 'secure the enterprise, secure the network,' which is essentially what we talk about as 'zero trust' today. I know what it took for us to do that."**
>
> **Jennifer Kron**
> Chief Financial Manager, National Security Agency

CIOs from across the IC said zero-trust implementation is critical to strong cybersecurity in the interest of national security. National Security Agency Chief Financial Manager Jennifer Kron, who previously served as deputy CIO, said the Defense Industrial Base plays a key part in cybersecurity, while Central Intelligence Agency CIO Ryon Klotz said the IC needs to be up to date on zero trust.

"Developing a common understanding of a basic maturity model for zero trust allows us to commonly evaluate where we are on the various pillars of zero trust and then target investments to enhance the maturity across [the IC]," said Klotz.

03
AI is integral to defending an ever-expanding attack surface.

Brian "Stretch" Meyer, senior director of field engineering at Axonius Federal, said he sees the future of cybersecurity focusing on expanding attack surface management beyond devices to include assets and leveraging AI for proactive threat detection.

"With AI and a human together, there's going to be a lot of future and that's going to really help drive when AI is tying into these tools," said Meyer. "The fundamentals of correlating the data together and looking at it that way is something that the industry just hasn't been in the habit of doing, and it's been eye opening when they do start to do it."

04
Integrated cyber deterrence is critical to the intelligence mission.

The elements of the IC work together to share information and build cybersecurity across the enterprise. Integrating cyber defenses is key to the IC mission, said Defense Intelligence Agency (DIA) CISO Tim Sydnor and Senior Technical Advisor Stephen Kensinger

"It's the integration, and by that, I mean the partnerships that we have across our community, so intimately partnered with our IC, fellow agencies, our peers in that space," Sydnor told GovCIO Media & Research. "It's not just DIA, it's a reflection of how we are integrating across our community – across our DOD partners – to deliver capability."

05
The IC uses AI for enhanced intelligence operations.

Artificial intelligence is augmenting the way the IC is doing its job for collection, analysis and distribution of intelligence data. Office of the Chief of Naval Operations Intelligence Division CIO Christopher Page said AI gives the Navy an advantage by increasing the volume, variety, velocity and veracity of collected data.

"We're no longer limited to a single discipline," said Page. "We can work across all the intelligence collection disciplines, whether it's geospatial intelligence, signals intelligence or all the other things that we can do these days from the platforms."

READ MORE