

**Software**

**Modernization**

**for**

**INFORMATION**

**Dominance**

**INSIDE:**

- Software Factories and Zero Trust ..... 3
- Graphic: Delivering Resilient Software for Comp. Advantage ..... 9
- Managing Open-Source Code Risk ..... 15

SPONSORED BY



# From the writer's desk




Kate Macri, Deputy Editor

## Software Factories Enable Information Dominance

**D**eputy Secretary of Defense Kathleen Hicks called for a “department-wide software factory ecosystem” in the Defense Department’s February 2022 software modernization strategy, elevating software factories as the harbingers of defense tech modernization.

For years, DOD software factories have relied on DevSecOps practices to quickly improve weapons systems and warfighter agility in an increasingly digitized geopolitical ecosystem to establish information dominance and seamless data interoperability.

Now, senior defense leadership is recognizing the role software modernization will play in the Joint All-Domain Command-and-Control initiative (JADC2), the recently awarded Joint Warfighting Cloud Capability (JWCC) contract, and the future of national security and cybersecurity.

Software factories paved the way to zero trust, mitigated the Log4Shell cyber vulnerability before it compromised sensitive data, and innovated API development for JADC2. What will they do next? 

# Table of Contents



Amy Kluber,  
Editor-in-Chief



Kate Macri  
Deputy Editor



Anastasia Obis,  
Staff Writer/  
Researcher

ARTICLE

## **How Software Factories Helped Pave the Way to Zero Trust**

Cultural and technical agility underpins the Air Force's new zero trust roadmap amid Defense Department zero trust activities.

BY KATE MACRI AND AMY KLUBER

INFOGRAPHIC

## **Delivering Resilient Software for Competitive Advantage**

A software development ecosystem allows the Pentagon to provide rapid software solutions to the warfighter at the tactical edge.

PARTNER INTERVIEW

## **Software Modernization Starts with Data Management**

Decision and information dominance starts with a critical look at the data and software solutions supporting it.

**Matthew Rose, Global Public Sector Industry Principal, Snowflake**

ARTICLE

## **How Army Software Factory Manages Open-Source Code Security Risks**

Securing open-source software is a unique challenge, and the federal government is just starting to develop ways to evaluate and minimize security risks associated with its use.

BY ANASTASIA OBIS

## How Software Factories Helped Pave the Way to Zero Trust

Cultural and technical agility underpins the Air Force's new zero trust roadmap amid Defense Department zero trust activities.

BY KATE MACRI AND AMY KLUBER

Software factories helped pave the way for the Department of the Air Force's new zero trust implementation roadmap, a quarter-by-quarter plan with a head start on the Pentagon's recently released five-year zero trust strategy.

The new roadmap, released Feb. 17, builds upon the service's zero trust strategy and identity, credential and access management (ICAM) roadmap released the same day.

"The Department of the Air Force, I believe, was the first in the DOD to publish a zero trust strategy and an ICAM strategy, so we've been working on our zero trust journey for a little while," Air Force CIO Lauren Knausenberger said in a recent GovCast interview. "We have some pretty good pilots in place and have worked from the beginning with sharing that knowledge and sharing that advocacy across the DOD, and so we participated in [producing] the DOD zero trust strategy."



Similar to the DOD's five-year strategy, the Air Force's zero trust roadmap spearheads the zero trust approach with multiple lines of effort: applications, networks, devices, users and data.

Conducting application inventory and integrating those into ICAM, secure access server edge (SASE) and software-defined perimeter (SDP) solutions will be the first big hurdle, Air Force CTO Jay Bonci told GovCIO Media & Research in an interview.

"We know that this is a long pole in the tent, but is the major early value in our zero trust architectural efforts," he said. "We have a lot of experience with this value stream in Cloud One, but those are applications that know they need to be modernized and refactored to move to cloud. Elements on premise that are in the 'retain' cloud category are going to be challenging and we don't have our hands around that just yet."

Cyber leaders across industry, defense and civilian agencies share Bonci's



perspective: knowing what is connected to your network and why, whether it be users, devices or applications, is critical for good cybersecurity.

“If you don’t know how to structure your protection mechanisms, if you don’t know how to structure the information you want to exchange, you’re not going to have an idea how to budget design or protection,” said Jay Gazlay, associate director for vulnerability management at the Cybersecurity and Infrastructure Security Agency (CISA), during a GovCIO Media & Research event in September 2022.

### **Software Factories Leading the Way**

The Air Force’s head start on zero trust is partly attributable to the cultural and technical agility cultivated over the last several years.

“Roadmapping allows us to create a granularity floor to talk about and show progress across these very complicated topics. It also enables for teams who are working on one slice of the picture — say, end-user devices — to know where those efforts need to link up with other parts, such as the universe of policy enforcement points,” Bonci said. “This has been in motion for many years now and our efforts stand on the shoulders of some of the early pioneers in the department who got these dominos moving. The roadmap documents those efforts and unifies them into a place where we can start to spot dependency and priority problems on a macro level, and we have hooked in most of our IT delivery teams into the creation and updating of these roadmaps.”

Software factories, in particular, helped transform the department into an organization primed to adopt a zero trust approach through DevSecOps principles, which will be important for securing the Advanced Battle Management System (ABMS), the Air Force’s contribution to DOD’s Joint All-Domain Command-and-Control (JADC2) initiative.

“Software factories are great for many reasons — for one, they allow us to move and prototype things very quickly,” Bonci said. “Many of the early zero

trust component implementations came out of Cloud One and Platform One. They have also been eager to help us get our hands around some particularly snarly problems. Deployable ICAM is one such problem set, and having cultural and technical agility in the factories in our consumers is going to be key to getting this right for ABMS. Based on that agility and a defined product market fit, the enterprise can do what it does best, which is scale this out to the entire Air Force in a cost-efficient manner. It has been a great partnership with those programs and platforms and we want to be doing more of that kind of rapid learning in the future.”

In the Pentagon’s five-year zero trust strategy, DOD CIO John Sherman said creating a zero trust culture is a No. 1 priority.

“This urgency means that our colleagues, our warfighters, and every member of DOD must adopt a zero trust mindset, regardless of whether they work in technology or cybersecurity or the human resource departments,” Sherman wrote in a foreword to the strategy. “This ‘never trust, always verify’ mindset requires us to take responsibility for the security of our devices, applications, assets and services; users are granted access to only the data they need and when needed.”

In order to attain the cultural sweet spot of understanding zero trust and its importance for maintaining effective cybersecurity in future fights, other service branches and DOD components should embrace technical agility, Bonci said.

“We are in a place in cyber history where risk of inaction has well overtopped the risk of action, and we as leaders must create places where we can experiment, make mistakes and re-vector as we learn,” Bonci said. “We have to do this with empathy and understanding that this topic is complex and that education and strategic messaging are key.”

Former Department of the Navy CIO Aaron Weis described a similar concept at the AFCEA West naval conference hosted by AFCEA International and the U.S. Naval Institute in San Diego this year: service branches should





**Jay Bonci**  
CTO, Department  
of the Air Force

consider cybersecurity as a problem of “readiness.”

DISA successfully completed its Thunderdome zero trust prototype pilot at the end of January and was issued a full authorization to operate, DISA’s Thunderdome Chief Engineer Julian Breyer told attendees at AFCEA West. Notable about the pilot is its potential to evolve and adapt along the way as it collaborates across other defense components working on zero trust implementation.

“The Thunderdome prototype ... isn’t supposed to be the end-all-be-all for us,” Breyer said. “The adoption is really the hard part. Fielding a new capability on a network and getting it approved to operate is certainly not an easy feat within the DOD environment, but then to take a step back and to work out processes to encourage our user base to think through what level of conditional access is appropriate for a specific application.”

With Thunderdome, Breyer said DISA has onboarded around 1,500 users at three different DISA sites and is working on a conditional remote access pilot with the Army. It’s expected to conduct red team testing around April and begin SASE migration in May, he said.

“We’re still engaged in ongoing dialogue with the services, many of whom are trying out different technologies than the ones that we’ve chosen,” Breyer said. “There’s a pretty great exchange between the different services and the different [zero trust] teams to talk about what their solutions do maybe better than ours and what our solution does better than them.”

Angel Phaneuf, CISO at Army Software Factory, emphasized empathy and compassion when teaching team members to “think” with a zero trust mindset during a recent GovFocus interview with GovCIO Media & Research.

“Taking the time to talk with humans and say, hey, the human element of this is we want to keep you safe, it’s not that you did anything wrong by scaling back this access,” she said, referencing how ICAM solutions, a pillar of zero trust, can be more restrictive about users’ access to data.

(ctd.)



Just recently, the Marine Corps launched its first software factory with an aim of making every uniformed Marine able to solve a software problem. The software factory also helps address current workforce gaps at DOD.

“In a lot of ways the software factories absolutely represent the future of the Air Force in that they’re using Agile processes, they’re using modern tools, they are incredibly adaptable,” Knausenberger told GovCIO Media & Research.

## **APIs and SBOMs for JADC2**

The Air Force’s new zero trust roadmap also highlights application programming interfaces (APIs) and developing software bills of materials (SBOMs) as key cybersecurity priorities for fiscal year 2023.

According to the roadmap, the Air Force plans to publish an enterprise SBOM strategy in fourth quarter 2023. This plan also circles back to the leadership of software factories: both the Air Force BESPIN Software Factory and Army Software Factory consider SBOMs their bread and butter for good cybersecurity, according to interviews with GovCIO Media & Research.

APIs are especially important for JADC2. As with the cultural element, Air Force software factories and DevSecOps principles set the example for securing APIs within a zero trust framework.

“We need to think about how we consume APIs from cloud services and commercial software, and what best practices look like for APIs that we produce,” Bonci said. “API-sharing is a key foundation to JADC2 and information-sharing with partners and allies broadly. We’ll need to define the right enterprise services which make it easy for developers to produce scalable, easily-secured and stylistically similar APIs. This includes credential lifecycles and other technical, policy and business considerations. Many of the early implementations are embodied in our DevSecOps environments like Platform One, but we will need to extend that beyond those ecosystems.”

APIs also go hand-in-hand with optimal user experience while maintaining security.

“The ability to have a good user experience also lies within endpoint security, and so I believe that interoperability is key to that, and API-enabled capabilities are key,” said DISA Senior Cyber Strategist Gillian Busick at the AFCEA West conference.

“If the DOD365 delivers some of our capabilities, and we’re delivering some of them in Thunderdome, and DoDNet delivers some of them for the Fourth Estate users’ desktop experience, all of that needs to be patched together, and so open API support is vital for that,” added Breyer at the conference. 🌟



**“Software factories are great for many reasons — for one, they allow us to move and prototype things very quickly. Many of the early zero trust component implementations came out of Cloud One and Platform One. They have also been eager to help us get our hands around some particularly snarly problems.”**

**— Jay Bonci, CTO, Department of the Air Force**

# Delivering Resilient Software for Competitive Advantage

A software development ecosystem allows the Pentagon to provide rapid software solutions to the warfighter at the tactical edge. **Transforming software delivery includes:**



**MULTI-CLOUD,  
MULTI-VENDOR  
ECOSYSTEM**

To access cloud at all classification levels

**DEPARTMENT-WIDE  
SOFTWARE FACTORY  
ECOSYSTEM**

To support warfighter needs at the speed of mission

**POLICIES AND  
PROCESSES  
TRANSFORMATION**


To create a shift in mindset and reach the full potential of software modernization

PARTNER INTERVIEW



# Modernization Starts with Data Management

Decision and information dominance starts with a critical look at the data and software solutions supporting it.

 **How do data sharing and collaboration tie into the Defense Department's JADC2 concept? What are some of the strategic and tactical or user considerations that are required for project success and overall decision dominance success?**

**Rose** Data is not only the foundation of Joint All-Domain Command-and-Control (JADC2), but also other U.S. allied and partner concepts such as NATO's Multi-Domain Command-and-Control or the U.K.'s Multi-Domain Integration. There are a few important commonalities between these concepts.

First, the data layer must be normalized for both complexity and volume. Second, the data required for JADC2 operations, decision frameworks, applications and advanced analytics/artificial intelligence (AI) relies upon systems and partners that are different from operations in the past. Third, legacy technology designs, architectures and methods will not achieve the flexibility, machine speed and fine-grained access control in a contested environment.

Practitioners, partners and leaders will benefit from revisiting their assumptions when planning their strategic guidance documents, plans and acquisition strategies. For example, the legacy approach to moving and copying data across network boundaries will not



**Matthew Rose**  
Global Public Sector  
Industry Principal,  
Snowflake

**“Platforms and solutions enabling the exchange of data across cloud providers while reducing friction for user experience is a winning approach. An example of this in action would be: a data scientist or analyst receives a notification when a dataset changes, or a recommender engine highlights other related datasets they can request access to.”**

**— Matthew Rose, Global Public Sector Industry Principal, Snowflake**

achieve performance benchmarks, security assurance and policy enforcement. Architectures such as object storage coupled with cloud elasticity is required for JADC2. There is not enough storage or funding available for approaches where we haul data across networks; rather, the workloads and compute will need to move to where the data resides.


 **What are some challenges to improved data visibility and interoperability that can hinder targeted software modernization efforts for cloud solutions?**

**Rose** Words such as interoperability, visible, joint, standardized, linked and trustworthy are used throughout DOD and other federal agency strategies. These terms convey a few common themes relating to technology and highlight not only the challenges, but also where friction is likely to occur.

Legacy infrastructure, changing operations models, talent management and the market are some of the reasons why organizations have not created an homogeneous single cloud architecture. Nor would a single cloud architecture be ideal from an industrial-base resiliency perspective. The recent Joint Warfighting Cloud Capability (JWCC) contract was awarded to four big cloud providers. We can expect that there will be a growing mixture of solutions up and down the technology stack.

Therefore, platforms and solutions enabling the exchange of data across cloud providers while reducing friction for user experience is a winning approach. An example of this in action would be: a data scientist or analyst receives a notification when a dataset changes, or a recommender engine highlights other related datasets they can request access to. Or, a platform offers the flexibility to translate, optimize and manage queries regardless of skill or language.

(ctd.)

 **The White House released its National Cybersecurity Strategy in March 2023, and agencies are now aligning their enterprises. How does this strategy and zero trust affect SaaS offerings and DevSecOps approaches?**

**Rose** The first National Cybersecurity Strategy codifies years of work conducted by the public sector, industry and academia. The stated goal is to enable a safe and secure digital ecosystem for all Americans. The strategy highlights how end users routinely bear too much responsibility for security, and the market — at times — does not incentivize security.

I expect to see “secure by design,” start to become a market requirement solutions must design for and incorporate zero trust principles from the beginning. These include things such as data encrypted both at rest and in transit, or workloads protected against unintended or unauthorized access. In that vein, the path by which the solution is brought to a user does not matter. I think the idea that the only way to achieve secure government systems is by building the solutions within government has been proven inaccurate. It is costly to build and maintain. Also, I do not believe it aligns with the intent of the strategy.”

I am also seeing a trend across all industries and markets where the legacy solutions are not able to achieve end states such as fine-grained access control at scale. This strategy and the expectations of users are fueling innovation.

(ctd.)





**What are you noticing in other industries and markets that will affect DOD in terms of data or AI?**

**Rose** Across the globe, I am noticing three specific trends emerging within the public sector, related industries and markets where data is mobilized. The first is the transition of data from a liability to an asset. I think the adage that data is the new oil is both incorrect and creates bias in our minds. Data does not lose value after being used once, but it is also expensive to hold, secure and maintain. Successful organizations are transforming their data from being a cost-driver into a profit-driver.

Governments and their citizens have also realized the importance and value of their data. As data collaboration matures, government regulators and technologists are addressing the importance of data by creating regulatory frameworks through which new markets, businesses, research, public services and international relations methods will emerge.

Finally, the third trend is the speed at which “disruptive” innovations has been proven inaccurate. It is cost to build and maintain. Also, I do not believe it aligns with the intent of the strategy.” innovations are not just related to technologies, but also include business models, research, services and policy. Early-adopter organizations find themselves buying down operational and technical debt while also creating value for their sector constituents and unlocking new opportunities. ✨



# SNOWFLAKE DATA CLOUD: ENABLING DECISION DOMINANCE

[snowflake.com/public-sector](https://snowflake.com/public-sector)

VIDEO



SOLUTIONS  
BRIEF



INDUSTRY  
BRIEF



JADC 2



## How Army Software Factory Manages Open-Source Code Security Risks

Securing open-source software is a unique challenge, and the federal government is just starting to develop ways to evaluate and minimize security risks associated with its use.

BY ANASTASIA OBIS

Army Software Factory is focused on teaching soldiers proper software security practices as the organization and others across the Defense Department ecosystem increasingly rely on open-source code, which can be a significant cybersecurity risk, as demonstrated by recent high-profile cyber incidents such as Log4j, which Army Software Factory mitigated within 24 hours of discovery.

According to the 2022 Synopsys Open Source Security and Risk Analysis report, 97% of analyzed codebases contain open source code. Sen. Gary Peters (D-Mich.) and Sen. Rob Portman (R-Ohio) introduced the Securing Open Source Software Act last year, which would direct CISA on how to minimize risk in systems that rely on open source code.

The legislation gives CISA a year to publish an open-source code risk framework and directs the agency to support supply chain security efforts.

“We used to have a battle about, you know, open source versus proprietary code, and, of course, it’s no longer a battle; they’ve both become synonymous,” Allan Friedman, CISA senior advisor and strategist, said during a recent CSIS Government Policies for Open Source Software panel. “And open source is a critical part of the organization, of the ecosystem that we have today. ... But, of course, we’ve started to pay attention to something that is not a new issue, which is, hey, is the stuff we are using actually secure? And even defining that is tricky.”

As DOD implements its software modernization strategy, which calls for a



“department-wide software factory ecosystem,” Army Software Factory frequently discusses the importance of understanding secure code with its cohorts.

“As we are training these soldiers to read and write code and understand it, we are also baking in how to do it securely,” Army Software Factory CISO Angel Phaneuf told GovCIO Media & Research. “You can write a piece of code that is not necessarily secure and that might not matter, but when you’re designing systems that our warfighters are going to be using, it’s so important that we



# Cap. Sidney Hall

Software Engineer,  
Army Futures Command



teach why code security is important,” Angel Phaneuf, Army Software Factory CISO told GovCIO Media & Research last year.

Army Futures Command founded Army Software Factory in 2021 to teach soldiers to write code and fill in software gaps they might encounter in theater.

Prior to the organization’s conception, the idea of soldiers spending their spare time learning technical proficiency and building applications was hard to imagine for senior leaders. But soldiers were able to demonstrate they did not need to rely on outside organizations to build software for them.

Since its founding in January 2021, Army Software Factory has built around 15 different applications and garnered nearly 30,000 users.

“It’s definitely something that is shifting and changing, the way that the Department of Defense thinks about software, as well as it’s certainly enriching the lives of soldiers, both those who are receiving the products that we build, as well as the soldiers that are coming here to the software factory to write code for their fellow soldiers,” Capt. Sidney Hall, a software engineer at Army Futures Command, told GovCIO Media & Research in an interview.

Hall was a member of the first cohort of soldiers when the factory launched. Within six months, they got applications into production in minimal viable form, solving problems soldiers were facing on the ground. From there, the factory iterated and pushed code and features out in a matter of days, sometimes hours.

“We’ve sped up our processes from years ... that are old, waterfall-like processes, and then using more agile-like processes in this organization. We are able to get code into production in the matter of months and then update and push a new feature pretty much in a matter of days,” Hall said.

Soldiers across the force can nominate an Army problem in need of a software resolution, such as a technical problem or an enterprise issue. If an idea shows promise, a team is sent to the site to ensure developers understand the issue, and then developers get to work.

One of the examples of an application developed at the factory is the PMCS

app used to help soldiers maintain their vehicles. Previously, the entire process was conducted on paper. “You lose a piece of paper, all the maintenance records are lost,” Hall said. Now, soldiers are able to access the application off of their phones to conduct vehicle maintenance.

The way the factory vets its software is the soldiers poke around to see if there is an existing solution to the problem they are trying to resolve, look further into where the software was made, when was the last time it was contributed to, and if it is being actively updated. They then move it to the platform security team with its own processes. The entire process takes about two weeks to assess whether the soldiers have access to and are able to incorporate a specific tool.

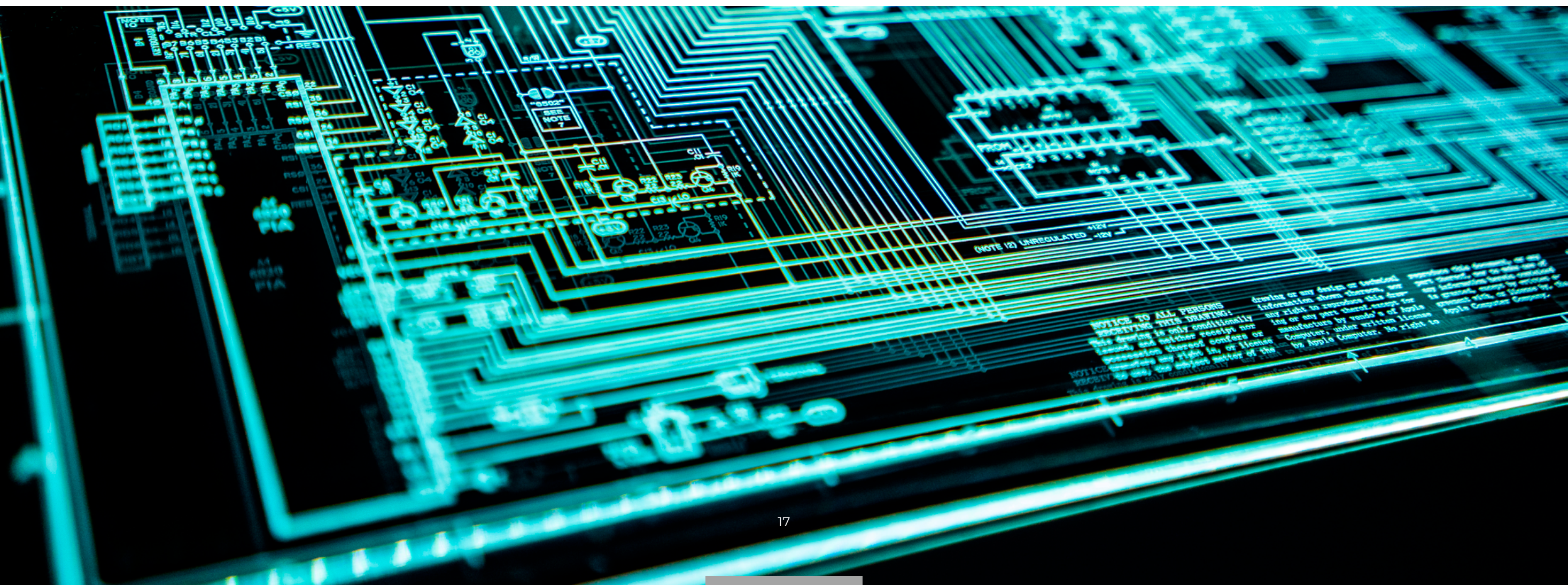
“There are some inherent risks using open-source software. There is the idea that, okay, you can see the source code, though, does it make it more vulnerable? But also, there’s more eyes on the code, so there is possibly more

contributions to make the code less vulnerable. ... The process of scanning and ensuring that there are little to no vulnerabilities in the code is of the utmost priority,” Hall said.

There have been numerous incidents associated with the use of open-source software within government, a recent one revolving around Pushwoosh, a company claiming to be based in Maryland, California, and Washington, D.C., but actually headquartered in Novosibirsk, Russia, according to Reuters. The Army removed the app containing Pushwoosh code last year, citing security concerns.

“[Defense Digital Service] still plans to use open-source software. We presume that the reason the Pushwoosh incident was found was because it was open source — it was there to discover. The quicker we know about a problem, the faster we can fix it. If Pushwoosh had been closed-source, how much longer would it have taken to discover the problem?” Nicole Thomson at the Defense

Photo Credit:  
Adi Goldstein on Unsplash



**“It’s definitely something that is shifting and changing, the way that the Department of Defense thinks about software, as well as it’s certainly enriching the lives of soldiers, both those who are receiving the products that we build, as well as the soldiers that are coming here to the software factory to write code for their fellow soldiers.”**

**— Capt. Sidney Hall, Software Engineer, Army Futures Command**

Digital Service told GovCIO Media & Research. “[The open-source software community] is a cultural tenet of DDS. We open source many of our products, and our employees also contribute to open-source projects.”

Hall said one of the techniques they use at Army Software Factory to mitigate risks associated with open-source software is to ensure it is not pulled directly from the internet. They take a snapshot of a piece of software, scan it, and store it in an Artifactory to ensure they have a clean build for app teams to be able to use it. Automation scans code and pushes it into production. Lastly, the factory’s security team always looks out for new CVEs. If a new version of CVE is released, teams are responsible for updating and patching that software.

“We’ve got some success stories where we’ve had teams go and patch a major vulnerability ... as fast as 8 minutes. On average, 24 hours is the rate at which we’ll patch software,” Hall said.

Top cybersecurity priorities at Army Software Factory in 2023 include developing a software bill of materials (SBOM), responding quickly to breaches and software vulnerabilities, and improving how quickly soldiers identify an alternate version or an entirely different piece of software to replace it. Another area of focus will be implementing the Pentagon’s five-year zero trust strategy.

“Having kind of like an Artifactory or some tool that stores our clean unsecure builds or software that we use here, so we know where all of our dependencies are coming from,” Hall said. “We can manage those, update them as we need to, get rid of them if we identify they’ve gone stale.” ❁