GovCIO
MEDIA & RESEARCH

DeepDives

DevSecOps & Cybersecurity

INSIDE:

SPONSORED BY

Invicti

GovCIO
MEDIA & RESEARCH

From the editor's desk

Amy Kluber, Editor-in-Chief

Baked-In Security

DevSecOps bakes in security at all aspects of a software development cycle — a key driver for robust cybersecurity strategies.

Culture is perhaps the most challenging component of DevSecOps. Leaders at the Defense Department, for example, say it's an all-hands effort and requires careful balance of the workload to prioritize capabilities. At U.S. Citizenship and Immigration Services, a modernized approach includes automating known risks and enabling teams to focus "manual" efforts on the unknown.

At its core, the digital landscape is evolving and teams need to adapt their cybersecurity tools and strategies accordingly.

Table of Contents

Nikki Henderson, Staff Writer

Kate Macri, Senior Staff Writer

GovCIO
MEDIA & RESEARCH

DevSecOps Movement Expanding Rapidly Throughout DOD

The Army, Air Force and Navy's modern application practices are improving security postures.

BY NIKKI HENDERSON

DevSecOps helps military service branches and the Department of Homeland Security (DHS) secure software applications against software vulnerabilities like Log4j, but prioritization is still a challenge as software development ramps up.

Approaching software development from a security-first mindset can be a difficult culture transition for some teams. A helpful tool for the Army Software Factory is the Army's DevSecOps playbook.

Army Futures Command's Software Factory in Austin, Texas.

Hannah Hunt, chief product and innovation officer at the Army Software Factory, said the factory recently launched its fifth application.

"The process itself is that we have security advocates whose sole job is to enable the success of the application teams to understand what security controls they need to maintain in order to go to production," Hunt said during an ATARC event. "There's a very tight feedback loop with security. They are developers with a security mindset so they know what needs to be built in order to be secure."

Matthew Huston, CISO for Platform One under the Air Force, said upskilling and empowering workers to handle modern software challenges helps position the Air Force with a stronger DevSecOps posture.

"As we've really been taking this DevSecOps movement the last five years, we have pulled up people from just coming in being basic engineers that had tremendous talent and then put them in key leadership positions to really help further along our efforts," Huston said. "We are also working with the DOD CIO office to establish different policies that we can push out and get the policies rewritten so they can support modern development."

DevSecOps has changed the way agencies develop security strategies.

United States Citizenship and Immigration Services (USCIS) approached DevSecOps from several different angles. First, the agency developed specialized information security officers embedded in their development

Photo Credit: Luke J. Allen / U.S. Army

Hannah Hunt

Chief Product and Innovation Officer, Army Software Factory

teams. These leaders were required to have backgrounds in coding and cloud plus accreditations in these areas.

Shane Barney, USCIS CISO, said the agency also gave development teams the ability to initiate things on their own and empowered them to deploy.

“We had to modernize our overall approach to cybersecurity, and we needed to stop focusing on known risks and automate those out of the way and start refocusing back on things we don’t know about, like SolarWinds, Log4j — because that’s where the ‘gotchas’ were going to come from and that’s where we were going to hurt,” he said during the ATARC event.

Leadership buy-in can make or break DevSecOps implementation plans. At the Air Force, consistent communication between software development and security teams and upper leadership is key.

“Getting leadership that understands what’s coming through, the security people understanding the developers, but then also the developers understanding what the security controls are and that way they can actually provide meaningful mitigations and I think that’s huge,” Huston said.

Zero trust principles also play an important role in DevSecOps implementation.

Ian Anderson, lead DevSecOps engineer of secure cloud architecture and automation at the Navy, said federal agencies should think about zero trust from the perspective of the end user.

“What does it need to do, does it need to read a file or does it need the more elevated admin privileges? It’s not just, ‘let’s implement this and everyone gets a key and it will authenticate,’” Anderson said. “You really have to look at it down to the permissions that these things need, so that way if something is compromised, you’re not giving away the whole network.”

The Army and the Air Force believe prioritization will be a major challenge

(ctd.)

> “We have security advocates whose sole job is to enable the success of the application teams to understand what security controls they need to maintain in order to go to production. … There’s a very tight feedback loop with security.”
>
> **Hannah Hunt, Chief Product and Innovation Officer, Army Software Factory**

they will both face in 2022.

“Radical prioritization is always a challenge,” Hunt said. “There are many fun and interesting things to do in the DevSecOps space, and you have to make sure your teams are not overwhelmed and can prioritize the workloads that will meet the users they intend to meet.”

Part of the prioritization challenge is sifting through emerging technologies and DevSecOps methods to identify ones that serve the mission.

“Prioritization is huge,” Huston said. “There are also still gaps that we’re looking to fill. We have developed many [continuous improvement] environments that are far superior to what our legacy processes were, but I think there is still more to come. I would love to see more chaos engineering and how we can automate that, more performance testing that we can embed in our different pipelines and help close the gap on some of the other feature sets that are great practices when it comes to software development.”

GovCIO MEDIA & RESEARCH

DeepDives

Secure Software Development

1

Protect the Software (PS):
Protect all components of the software from tampering and unauthorized access.

3

Respond to Vulnerabilities (RV):
Identify residual vulnerabilities in software releases and respond appropriately to address those vulnerabilities and prevent similar vulnerabilities from occurring in the future.

2

Prepare the Organization (PO):
Ensure that the organization's people, processes, and technology are prepared to perform secure software development at the organization level and, in some cases, for individual development groups or projects.

4

Produce Well-Secured Software (PW):
Produce well-secured software with minimal security vulnerabilities in its releases.

Source: NIST SP 800-218

PARTNER INTERVIEW

Security Best Practices in IT Modernization

The growing attack surface amid digital development environments requires honing in on security.

Sonali Shah, Chief Product Officer, Invicti

As agencies modernize systems and adopt more cloud-based tools, streamlined development and testing approaches ensure efficiency and security of those systems. With the attack surface only growing with the expansion of digital tools, securing every doorway to potential attacks is critical.

Invicti Chief Product Officer Sonali Shah discusses how automation, culture and DevSecOps can ensure software teams are leveraging the best security practices in their organizations.

What security approaches are necessary for application development and production?

Shah Every organization that builds and manages applications is a software company. In application security, it's crucial that companies do the following three things to ensure the maximum amount of risk reduction:

- Use tools that are accurate and automated. Inaccurate tools will result in a lack of trust among developers and make it difficult to get their buy-in. Without automation, you will never be able to scan and secure your entire attack surface.
- Shift left *and* right to continuously secure your applications, both in development and in production. Scan in development to fix vulnerabilities where they are cheapest to fix, and scan in production to catch new ones.
- Build a culture of security, including training your developers on secure coding practices and building internal security champions that promote knowledge sharing and collaboration between security and development teams.

(ctd.)

> “By fully integrating modern solutions and building security into their development processes from day one, agencies can catch more issues before they become costly and damaging.”
>
> —Sonali Shah, Chief Product Officer, Invicti

How does today’s modernization landscape impact how an organization should approach application security?

Shah Attack methods are ever evolving. What you think is secure today might not be secure tomorrow. This makes it tricky to stay ahead of every bad actor. This is also where modern security tools shine — helping government agencies that may have previously relied on antiquated tools and processes maintain continuous security coverage with the most accurate results possible.

Many organizations have gone through a digital transformation in recent years to modernize their approach to IT, including more robust security tools that plug into existing workflows and a shift to the cloud for greater agility. By fully integrating modern solutions and building security into their development processes from day one, agencies can catch more issues before they become costly and damaging.

How can DevSecOps impact and enable better software development?

Shah One of the core benefits of DevSecOps is that it helps unify development and security processes to ensure seamless coverage. This improves development speed and boosts security posture, while also saving agencies money as it reduces the overall costs of security operations. When driven by leadership with authoritative and clear direction, critical best practices are easier to follow and can help reduce stress for overworked teams.

DevSecOps is also about creating quality code and improving your software. Treat security like you would treat quality; test early and test often, automating as much of that process as possible and building it into your development pipeline. With DevSecOps, organizations are more likely to fall into the good habit of testing code for vulnerabilities well ahead of release, catching potential exploits before disaster strikes.

(ctd.)

```
elif _operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
```

What emerging technologies do you see impacting this space?

Shah Monolithic and legacy solutions are out, streamlined and modern tools are in. With emerging technologies like artificial intelligence (AI) and machine learning (ML) embedded into modern security solutions, we have the opportunity to vastly improve speed and accuracy in cybersecurity.

Cybersecurity is only at the cusp of grasping the full potential AI has to offer, but the benefits are clear: when embedded into scanning technologies, AI can be used to identify threats quickly, automate the prioritization of vulnerabilities and even estimate the risk and impact of a potential exploit. Ultimately, that means agencies of all sizes will have the opportunity to manage their risk of a data breach without constraining their resources or busting budgets.

Photo Credit: whiteMocca

DevSecOps is Essential For Good Cybersecurity

Defense leaders say nothing is more important to a sound cyber strategy than culture change.

BY KATE MACRI

For some branches of the military, a DevSecOps approach to cybersecurity is the best way to shield their networks from the onslaught of ransomware and cyberattacks from nation-state actors.

Cyber leaders from the Navy, Army, and Defense Information Systems Agency said their cyber strategies include multiple facets, such as Agile methodology and cultural overhaul, to maneuver the current cyber landscape.

“Over the years we’ve shifted from the bolt-on methodology to cybersecurity that’s baked in,” said Rear Adm. Susan BryerJoyner, director for the Navy’s cybersecurity division, during a GovConWire Cybersecurity in National Security event. “We’ve also done a change in our culture. Everybody has come to realize that cybersecurity is an all-hands effort. Do your part, be cyber smart.”

BryerJoyner said she’s focused on integrating cybersecurity into the Navy’s systems engineering in order to simplify cybersecurity processes. But new methodologies aren’t always enough. Sometimes the key to better cybersecurity lies in the tools you already have, Joyner said, such as data.

“The secret sauce is not in the data your tool is producing, it’s in the way your tool handles the data,” she said.

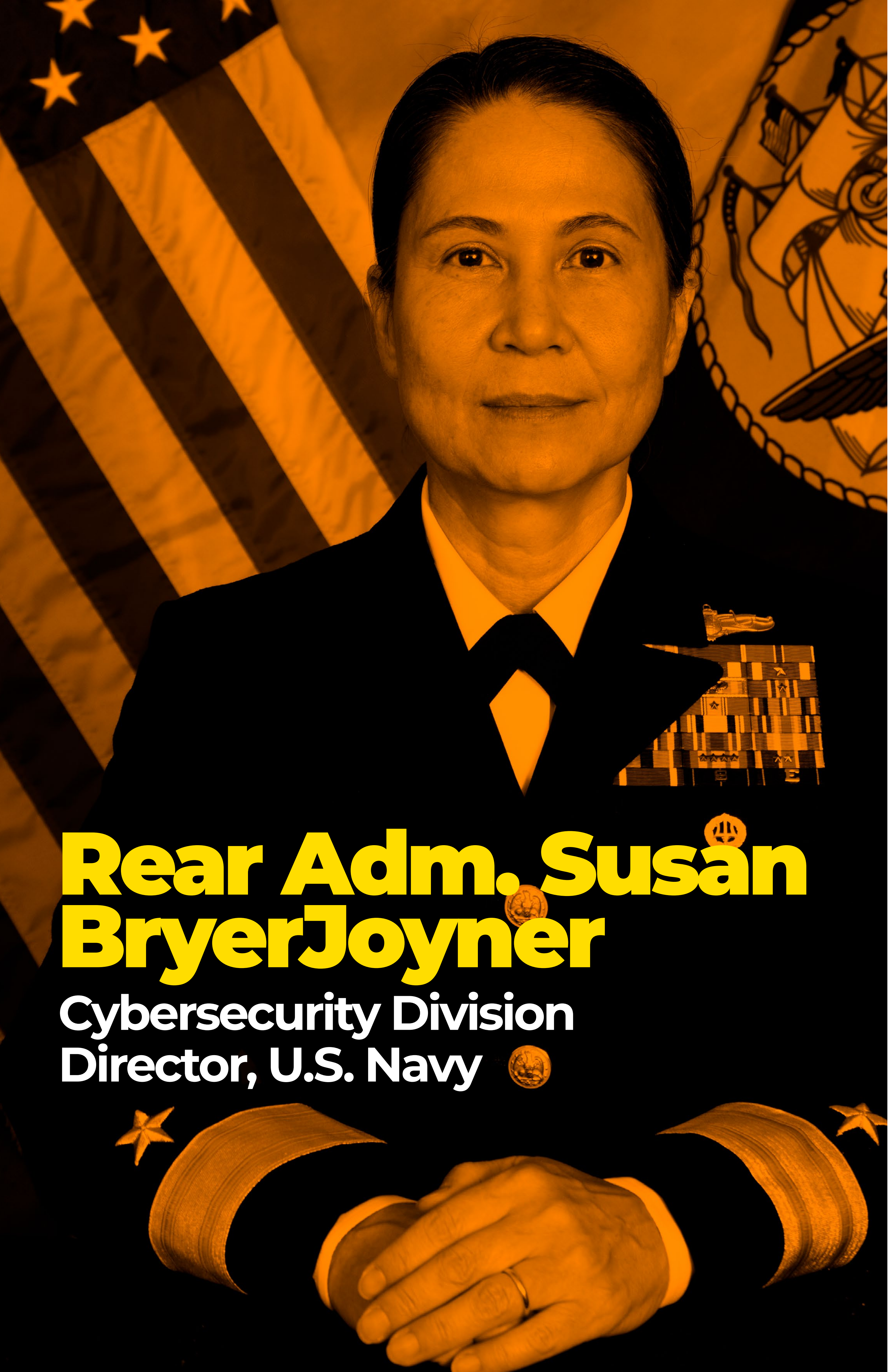
For example, the Navy uses data to analyze cyberattacks and help “properly defend” its networks against future attacks.

“At the end of the day, if we look at DevSecOps and that Agile approach to cybersecurity … we need to make sure they have data available to them, where it is, and how they can integrate those feeds into whatever function they’re trying to perform,” BryerJoyner said.

Early software testing, which is integral to DevSecOps, is a key component of the Department of the Navy Acting CISO Tony Plater’s cybersecurity strategy.

“I’m [also] focused a lot on interoperability and performance requirements,”

Photo Credit: saidka/iStock



Rear Adm. Susan BryerJoyner

Cybersecurity Division Director, U.S. Navy

he said at the event. “Previously we found when we had 100% coverage of cybersecurity requirements but terrible performance on our networks, that became a significant issue for our end users, the warfighter, the business unit.”

Compliance only goes so far if you’re still experiencing breaches, he said. So, Plater deprioritized compliance requirements and focused on cybersecurity performance instead.

“80% coverage with better performance is more of a viable path,” he said. “From a prioritizing perspective, we’re looking at how we do things differently. In many cases we knew what all the cybersecurity requirements were, and now we’re trying to change perspective, how does the adversary see our network and what can they get to? That’s one of our strategic initiatives … pivoting to readiness, rather than just compliance. We want to [be] data-driven, operations-relevant.”

For Matthew Easley, who was at the time the CISO and director of cybersecurity at the Department of the Army, balancing cybersecurity with IT modernization is his biggest challenge. Keeping his focus on the mission helps him balance these two priorities.

“We have to prioritize our cybersecurity requirements and really understand which ones are getting the most return on investment,” he said at the event. “We’re doing that with the rest of our cybersecurity community — what types of security controls are non-waivable? And which are waivable in certain circumstances? And do that in a cohesive manner and get better inheritance between security controls and what’s being provided by a network and weapons system platform.”

The shift to zero trust architecture helps simplify and streamline cybersecurity for the Army, he added.

“It’s really important that as we move into this new paradigm for cybersecurity and use software to identify networks and bring our own devices and use different techniques to defend endpoints, that we do that in a logical

(ctd.)

“If we look at DevSecOps and that Agile approach to cybersecurity ... we need to make sure they have data available to them, where it is, and how they can integrate those feeds into whatever function they’re trying to perform.”

Rear Adm. Susan BryerJoyner, Cybersecurity Division Director, U.S. Navy

manner and not use a one size fits all for a million endpoint users in the U.S. Army,” he said. “Certain categories will need a higher level of defense, and a little less defense at our newer soldiers coming into the formation.”

Implementing new cybersecurity methods requires cultural adaptability and resiliency, but the current cyber landscape also calls for a dash of realism: no one is safe, and everyone will suffer a cyberattack at some point.

“The biggest thing continues to be culture,” said DISA Director Lt. Gen. Robert Skinner. “How do you change the mindset of never letting anything in, to making sure that if you are breached, you have the right resiliency in place and other initiatives so that you limit the impact it does have? Because it will happen at some point.”

Skinner said email continues to be the No. 1 cyber risk for most federal agencies, including DOD. The best way to fight these cyber threats is through systemic cultural change.

“The culture of users and administrators [needs] to change from being a passive administrator to an active,” he said. “So how do you retrain and hold people accountable for breaches of cyber rules and guidance you have out? The whole notion of, if you get an email that says ‘free’ on it, to hold back the temptation of clicking on it. I know that’s hard, but the more we continue to innovate the more the culture will change.”