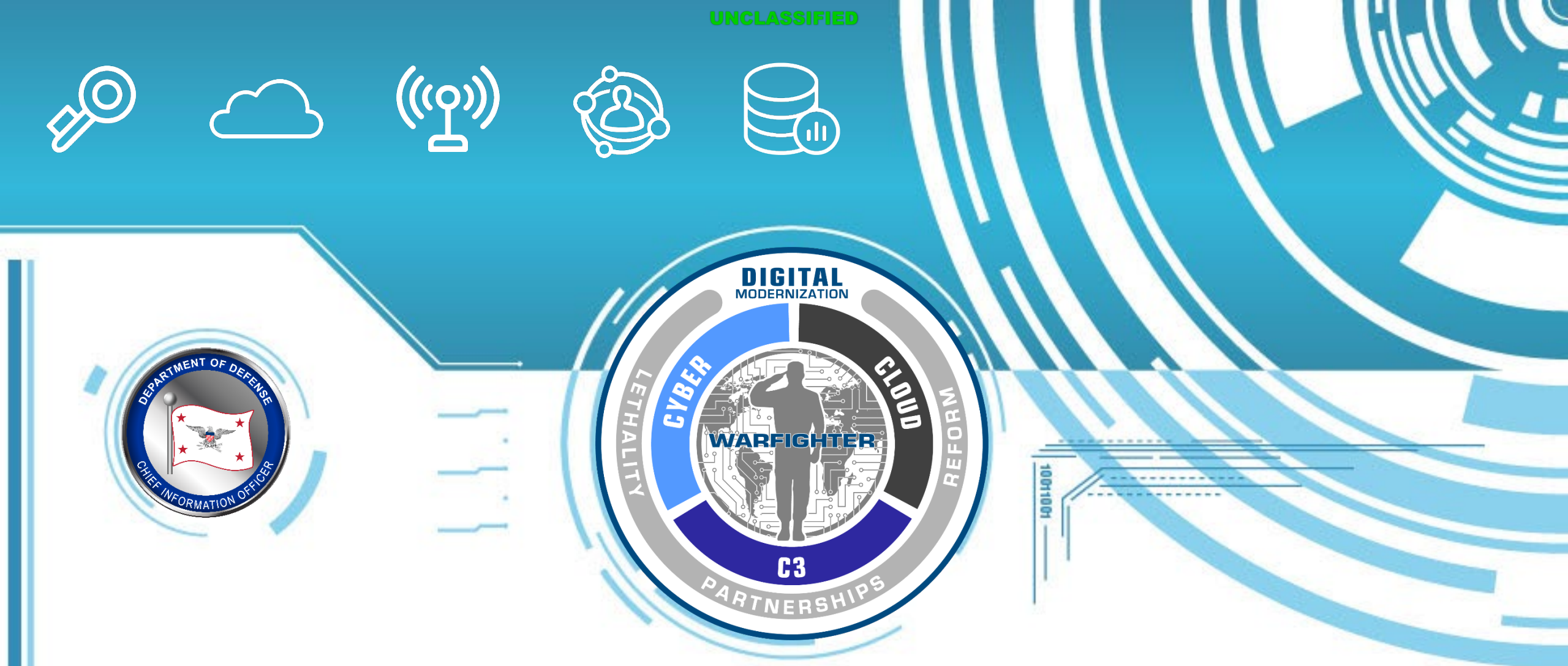


DoD Enterprise DevSecOps Community of Practice

August 11, 2022

Agenda

- Welcome
- Keynote:
  - Ms. Sarah Standard, OUSD (R&E); Developmental Test, Evaluation and Analysis(DTE&A) ,The Cybersecurity/Interoperability Technical Director
- “Cybersecurity Operational Test and Evaluation Concept for Software Factories”:
  - Dr. Billy Robbins, IDA, follow-on discussion with Ms. Sarah Standard, and Mr. Nilo Thomas, OSD DOTE, Software and Cyber Action Officer
- Q&A
- Intro to the Institute for Defense Analyses (IDA) Report:
  - Ms. Sarah Standard
- Cybersecurity and DoD System Development: A Survey of DoD Adoption of Best DevSecOps Practice:
  - Mr. Lee Kennedy, Mr. Steve Wartik, Mr. Ryan Wagner, and Ms. Rachel Kuzio de Naray, Institute for Defense Analyses
- Open Q&A

Cybersecurity and DoD System Development: A Survey of DoD Adoption of Best DevSecOps Practice

George “Lee” Kennedy
Ryan Wagner
Steven Wartik
Rachel Kuzio de Naray, Project Leader

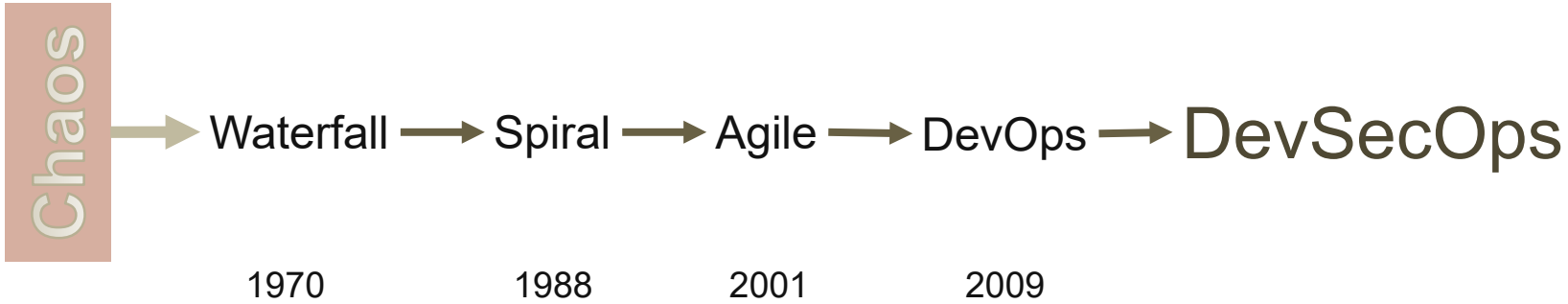
11 August 2022

Institute for Defense Analyses
730 East Glebe Road ● Alexandria, Virginia 22305

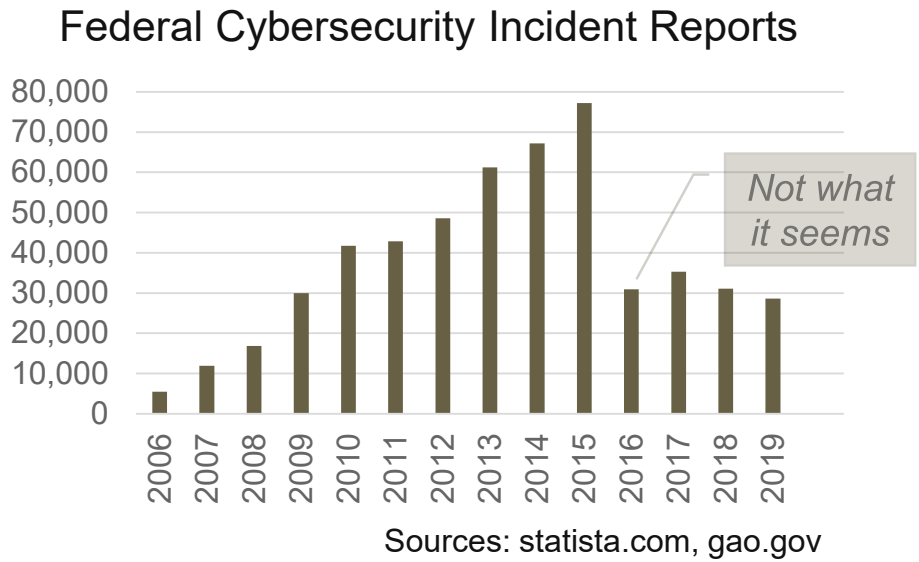
Outline

- Introduction
  - Background
  - Current Status
  - Methodology
- Responses
- Findings
- Recommendations and Conclusions

DevSecOps: A stage in the evolving software lifecycle

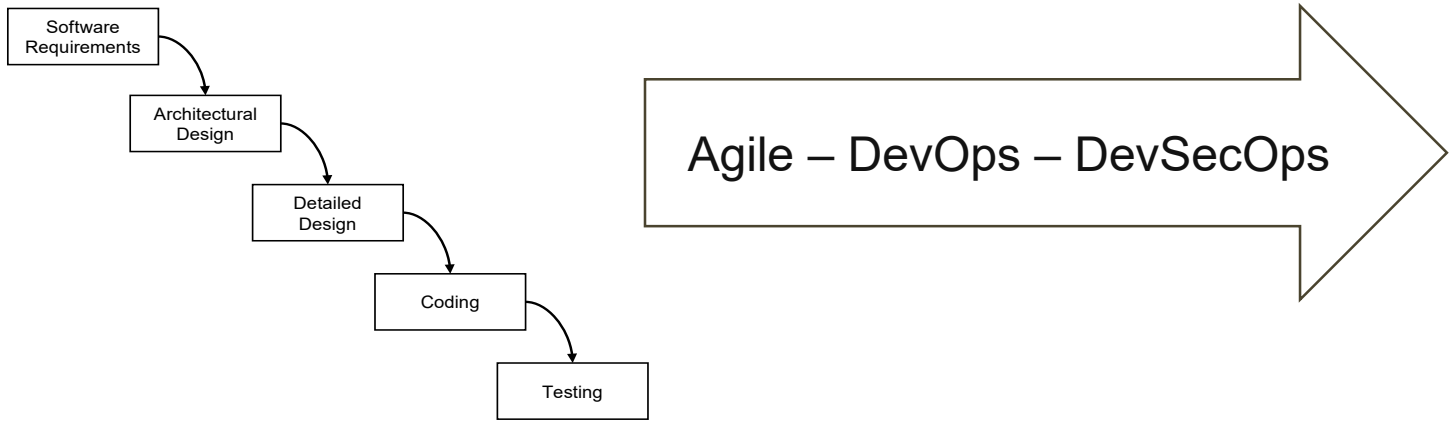


Meanwhile …



DoD needs to "shift security left"

What is the state of lifecycle models (especially DevSecOps) in DoD?



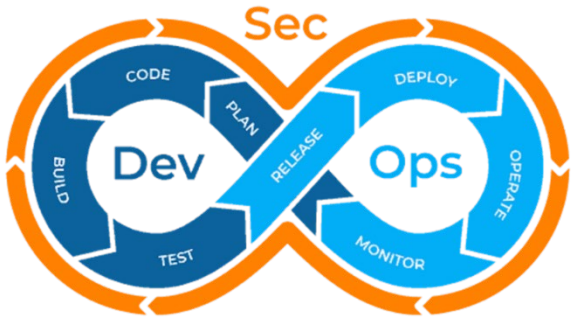
Are Agile, DevOps, and DevSecOps widely used?

- How are they being used?
  - Do documented policies, standards, and practices exist?
  - What tools are used (commonly or otherwise)?
  - What environments are used?
  - How is the need for developmental testing addressed?
- What success stories exist?
- Are there problems, and even failures?
- What lessons learned can be shared?

IDA's FY 2021 study of DevSecOps

- At direction of Cybersecurity/Interoperability Technical Director, USD R&E DTE&A, Sarah Standard, IDA studied DevSecOps (DSO) adoption in DoD

- The study consisted of:
  - Literature reviews
  - Surveys
  - (Virtual) Interviews



- IDA identified successes, challenges, and gaps

- Specific focus on integration of "Dev" cyber testing

- *This was not a comprehensive, DoD-wide survey*
  - *Research was significantly constrained by COVID restrictions and limited availability of participants*

Responses: What is DevSecOps?

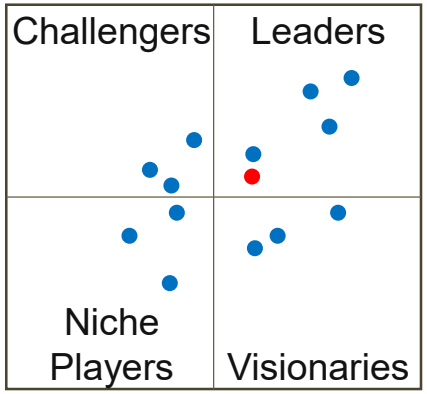
Agile? DevOps? DevSecOps?

- Surveys and interviews revealed confusion about Agile vs. DevOps vs. DevSecOps
  - DevOps is well-defined†, DevSecOps less so
- Examples:
  - Organization that “uses agile, with DevSecOps pipelines”
  - A developer wanted short spurts to minimize reboot time – but reboot time was irrelevant
  - One interviewee said in his group, each team had to figure out how to be agile and how to use a DevSecOp context for testing, but said he didn’t know how agile and DevSecOps differ
  - USAF often uses DevOps and DevSecOps interchangeably
  - A group that’s practicing DevSecOps isn’t sure who’s responsible for security

†The DevOps Handbook

Responses: Application Security Testing (AST)

- Respondents agree extensive AST is necessary for successful DevSecOps practice
- Gartner Group's "magic quadrant" shows:
  - 14 important commercial vendors of AST tools
  - 5 of these are industry leaders
- 8 respondents reported use of Fortify, SonarQube, or both (Static AST)



- Little use of Dynamic AST
- Some organizations automate AST as fully as possible
- Some aspects of AST can't be automated
- Determining where manual testing was required and integration of manual testing was challenging

Responses: Environments and Pipelines

- Organizations consistently use different environments for development, testing, staging, and deployment
- Organizations consistently use containers to manage environments
- Organizations use git repositories to assist with:
  - Component reuse
  - Version control
  - Configuration management
  - Automating pipelines
- Often, software is:
  - Developed in unclassified environment
  - Deployed in classified environment
- Stovepiped security testing
  - Too often confined to the application code
  - Ignores environment: pipeline itself, virtualized environment, containers, etc.

- Slow transfer from unclassified to classified environment hinders Continuous Delivery.
- Inability to host classified data in unclassified environment hinders debugging.

Responses: Program Management

- Respondents referenced leadership's lack of understanding of DSO strengths and limitations
- New, smaller, programs with less legacy baggage achieved the best results
- Level-setting by including program managers, developers, functional and security testers in training/team sessions from program initiation was an indicator of success
- Maintaining DSO success as programs scaled became difficult due to external constraints designed for waterfall methodologies (compliance with budget, RMF, acquisition and testing milestones)
- System security requirements were frequently not considered when developing test objectives – overreliance on commercially used and available automated code analysis products

Success of DSO efforts correlates to maturity of practice

Findings: Success stories

Success Stories	# of Responses
Enculturation of DevSecOps is foundational	8
Fully leverage automation for testing, pipeline, and builds	8
Incorporate test processes and environments up front	6
Results can be validated	4
DevSecOps can be adapted to physically isolated environments	2

Conclusion: Some respondents believed they had successfully adopted DevSecOps.

Not so fast …

- Remember, people confuse the methodologies
- There aren't 10 projects using DevSecOps

Findings: Problem Areas

Problem Areas	# of Responses
Many DoD systems may be incompatible with the DevSecOps process	6
The role of Developmental Testing (DT) within a DevSecOps methodology is unclear	6
The difficulties of classified versus unclassified DevSecOps development are unresolved	5
The current DoD Authority To Operate (ATO) process is not fully compatible with DevSecOps	4
There is no adequate standard definition of DevSecOps	4
Forming teams proved more challenging than expected	4
Organizations had trouble allocating resources	4
The current DoD acquisition model does not lend itself to a DevSecOps development methodology	3

Some respondents reported they would “fail back to waterfall.”

Findings: Lessons Learned

Lessons Learned	# of Responses
Automation is key	8
Security requirements need to be more mission-focused	7
Starting with DevSecOps is easier than switching to DevSecOps	6
DevSecOps must be adapted to the operational environment	6
Leverage good architecture and design to support security	6
DevSecOps is easier on small projects than big ones	5

Participants' experiences with DevSecOps reflect their environments, projects, resources, and familiarity with non-waterfall methods.

IDA's recommendations to DoD to promote DevSecOps

- IDA makes 12 recommendations

DoD-Wide	Per-Program (Managerial)	Per-Program (Technical)
Adopt standard definition of DevSecOps	Identify mission-focused security requirements	Use good development environment architecture
Create top-down understanding of DevSecOps concepts	Identify and use security metrics	Fully leverage automation
Adopt DevSecOps maturity model	Commit sufficient operational and security staff	Account for testing that can't be automated
Understand cultural and resource challenges in conversion	Ensure DevSecOps is appropriate	Use DoD enterprise code repositories

- IDA also recommends a follow-on study on how to implement Continuous Authority to Operate (cATO) under DevSecOps*

*The DoD CISO has recently published a cATO memo and is undertaking an effort to address this issue

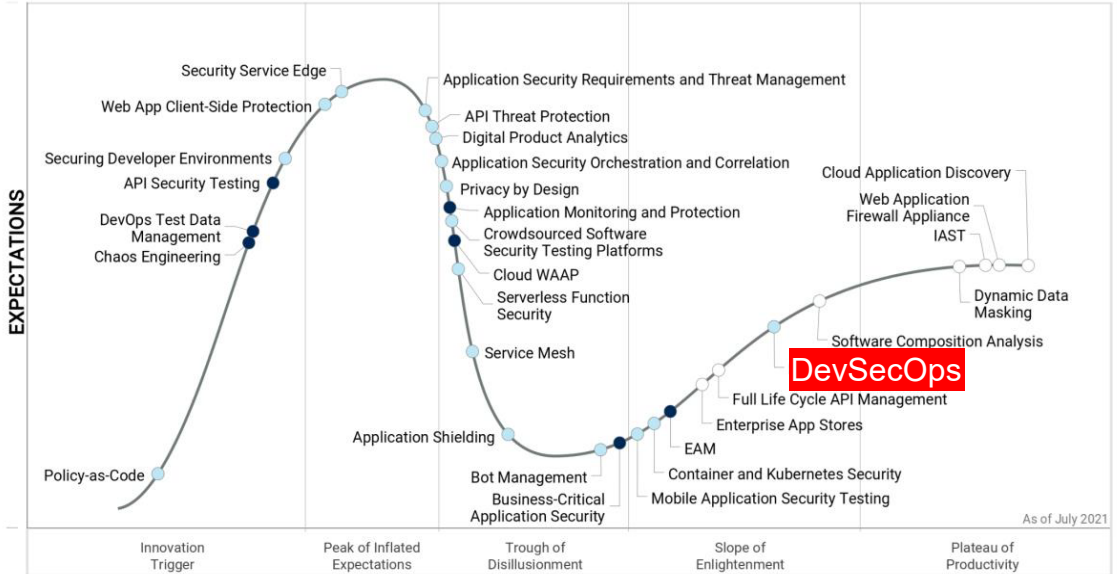
Conclusions

- DevSecOps has taken hold in DoD
- However, it is not yet pervasive or mature
- IDA identified 3 relevant maturity models:
  - Naval Information Warfare Center Atlantic
    - 9-level maturity model
  - DoD's DevSecOps maturity review
    - List of questions designed to elicit an organization's approach to DevSecOps and suggest improvements
  - OWASP DevSecOps Maturity Model
    - 4-level security-focused model

These aren't as rigorous as CMMI models, but IDA recommends them as a starting point.

Conclusions (cont'd)

- Regarding IDA's recommendations:
  - DoD-wide recommendations will take time
  - Implementing managerial and technical recommendations requires ongoing research
- DevSecOps is not a fully mature technology
- As of July 2021, Gartner Group predicts maturity in 2023
- DoD may lag due to problem areas noted by IDA



Backup

Reference Documents

- Documentation on service websites
  - USAF
  - Naval Information Warfare Center

  } *Of particular note*
- DoD Enterprise DevSecOps Reference Design
- Industry-published books
  - The Phoenix Project, The Unicorn Project
  - The DevOps Handbook
- NIST Special Publications and reports
  - Covers technologies important in DevSecOps, not DevSecOps itself
  - Security, automated testing, risk management
- Gartner Group reports

Surveys

- 24 questions, with mainly free-form answers
- Questions grouped into 5 categories:
  - ❑ Development processes
  - ❑ Development practices
  - ❑ Roles
  - ❑ Testing
  - ❑ General observations
- Distributed to 45 individuals in January 2021
- Received 10 responses, one of which had “N/A” for every question
- Given the organizational level of the respondents, negative responses are significant

Interviews

- 18 interviews conducted between March and June 2021
  - Survey and interview subjects sometimes overlapped

- Interviewees' affiliation:

Service	# of Interviews
Air Force	6
Space Force	4
Army	4
Navy (including USMC)	3
Other DoD	1

Interviews (cont'd)

- Interviewees' Roles:

Role	# of Interviews
Developer/Pipeline	6
Operational Test	4
Developmental Test	8

- The IDA findings and recommendations are based on these interviews and the indications in the DoD document reviews on the state of DSO practice in DoD
  - NOT commercial practice.

POC Information:

- **Sarah Standard** sarah.m.standard.civ@mail.mil OUSD (R&E); Developmental Test, Evaluation and Analysis (DTE&A) ,The Cybersecurity/Interoperability Technical Director
- **Nilo Thomas** nilo.a.thomas.civ@mail.mil Action Officer, OSD DOTE

Closing Comments:

Mr. George Lamb, Computer Scientist, Cloud and Software Modernization

Next CoP: Thursday 11 August, 1300-1600 ET