Checks and Balances

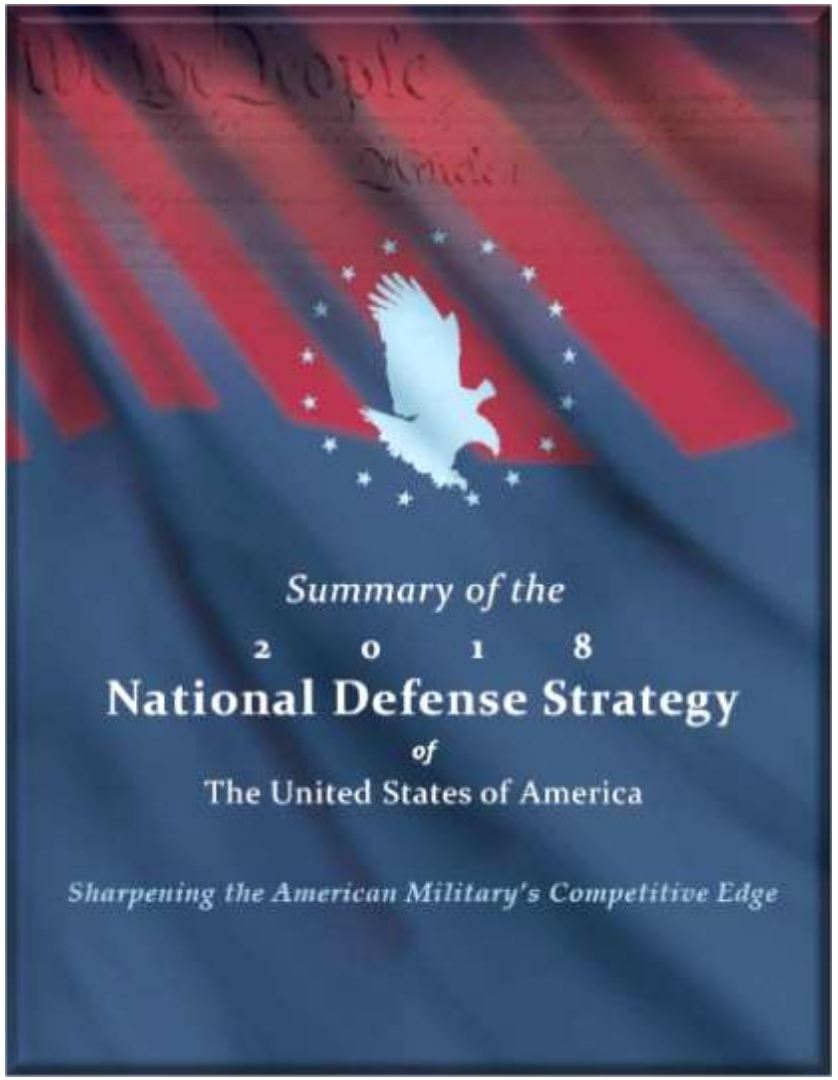
ISO
Joint Technical Exchange Group

29 Oct 19

JTEG Member Contribution

National Defense Strategy
January 2018

- The *National Defense Strategy* acknowledges an increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations.
  - SECDEF Mattis



January 2018

In 2018 what did DEPSECDEF task us to do?

DEPSECDEF Pat Shanahan: May 2018

- We think about China not just militarily, we use the term 'great power competition.'

- We see their growth in the military, their pursuit of predatory economics, their theft of intellectual property as disruptive and threatening to the American way of life.

"We will expand the competitive space while … reforming the Department's business practices for greater performance and affordability."

List of key technologies 2015:

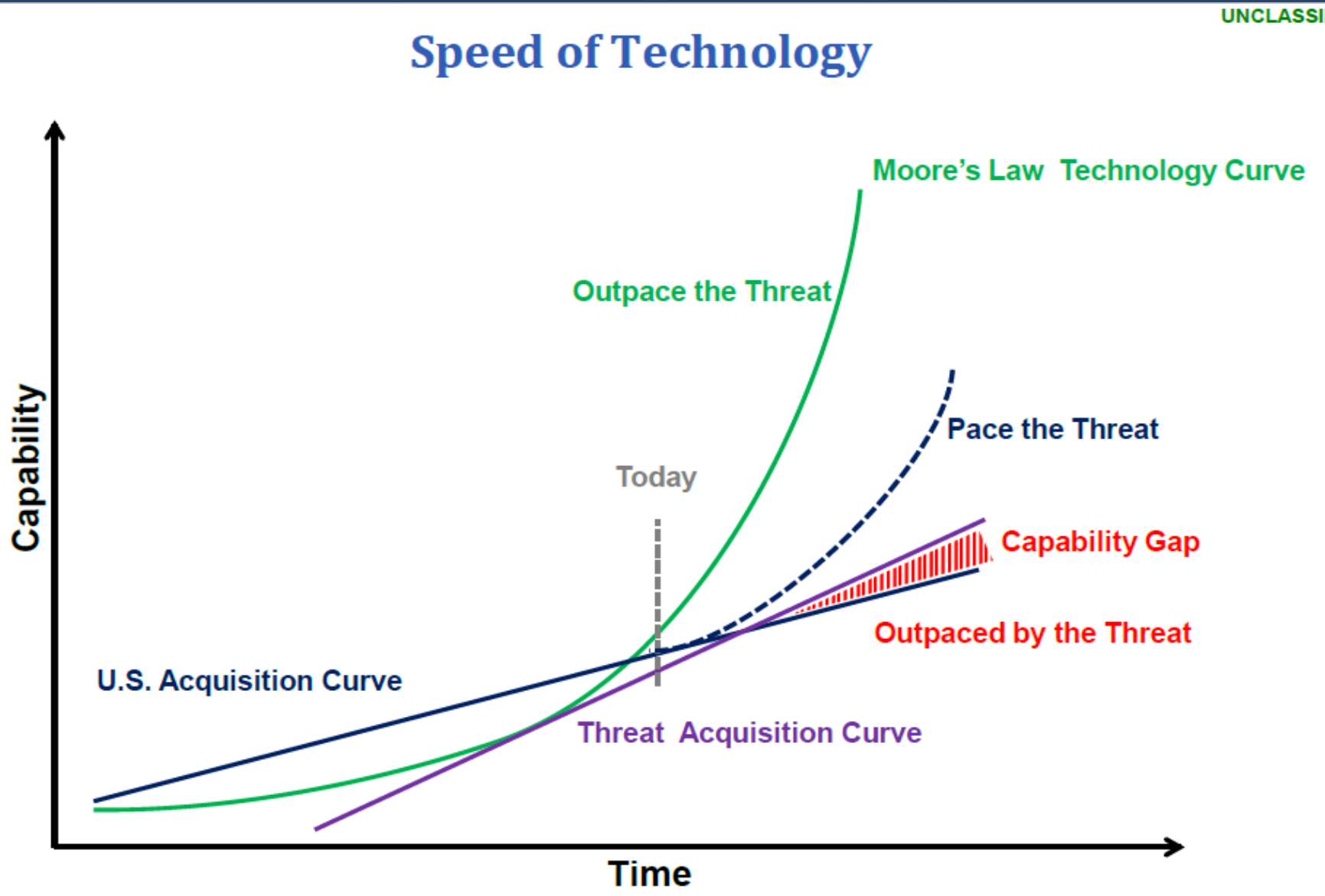
- Robotics
- Autonomous Vehicles
- Computer Visualization
- Big data
- Biotechnology
- Micro- miniaturization
- Advanced computing

List of key technologies 2018 (NDA):

- Robotics
- Autonomy
- Big Data Analytics
- Biotechnology
- Directed Energy
- Hypersonics
- Artificial Intelligence

Problem: Being Outpaced By the Threat

UNCLASSIFIED



Current System is too Slow

Innovation & Cybersecurity

Digital Innovation provides dynamic, multi-dimension challenges for those responsible for designing and implementing cybersecurity functions

- Vulnerabilities of adoption
- Threat posed by non-adoption
- Rate of change of technology
- Rate of obsolescence in DOD baseline
- Threat posed by ubiquitous access
- Obsolescence of workforce
- Depth of relative gap between DOD and competitor baselines
- Loss of situational awareness
- Complex Supply chain, operational value chain and labor-chain risk

The balance between Innovation and Security is defined in terms of the optimum speed for tech adoption (e.g., optimizing flow)

Risk

We are competing against time:

- ***FLOW*: The balance between Innovation and Security**
  - Defined in terms of the optimum speed for tech adoption

- ***Speed* becomes the number one Key Performance Parameter**
  - When (date)
  - How Long (date range)
  - When and How long in relation to competitors
  - When and How long in relation to combinations of technologies
  - When and How long in relation to DOD (blue) baseline

- **Theory of Constraints**
  - Cybersecurity requires we communicate in terms of ToC*
  - TECH-SEC tradeoffs are required to achieve mission outcomes

* Theory of Constraints: First described in "The Goal," Goldratt et al, 1985

Rip Van Winkle Syndrome

- Washington Irving: 1819
- 20 Year Slumber
- Loss of Situational Awareness, Relevance
- Post-AT&L era
  - A Response to 20 year period of acquisition "slumber"
- 2019-2025
  - Re-Orienting to era of Peer Competition

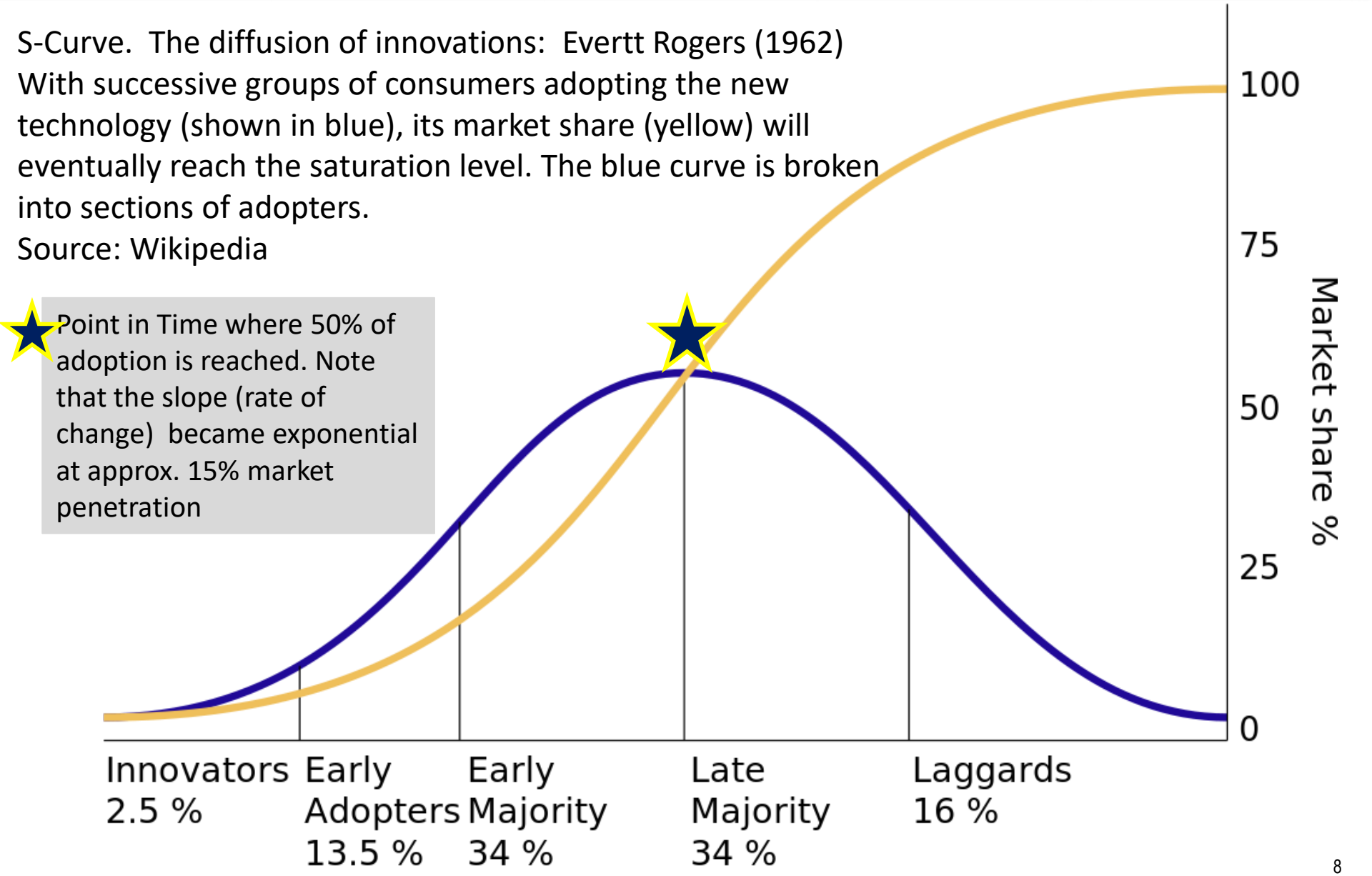
Joseph Jefferson as Rip Van Winkle (1896): Source Wikipedia

Many technologies appear new to DOD, but not to our competitors

Diffusion of Innovation

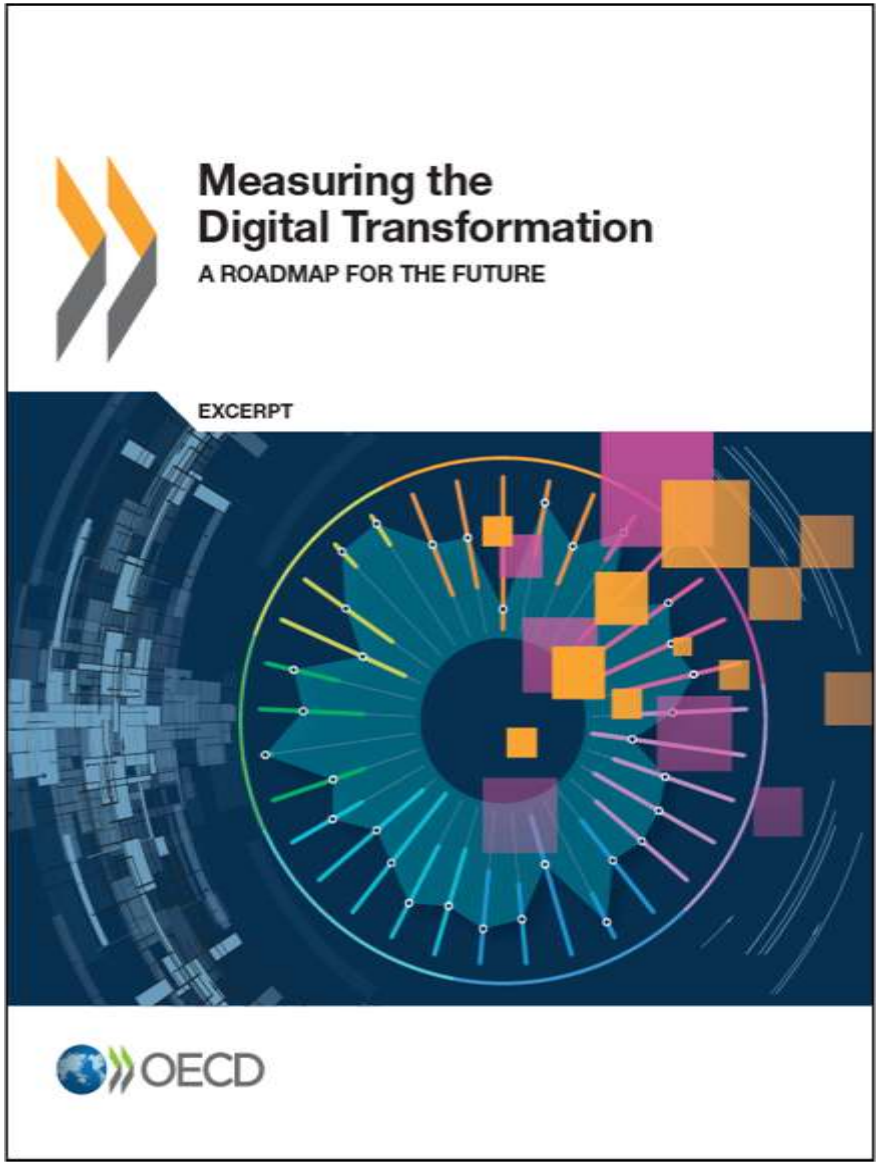
S-Curve. The diffusion of innovations: Evertt Rogers (1962) With successive groups of consumers adopting the new technology (shown in blue), its market share (yellow) will eventually reach the saturation level. The blue curve is broken into sections of adopters.
Source: Wikipedia

Point in Time where 50% of adoption is reached. Note that the slope (rate of change) became exponential at approx. 15% market penetration



You Can't Manage What you Can't Measure

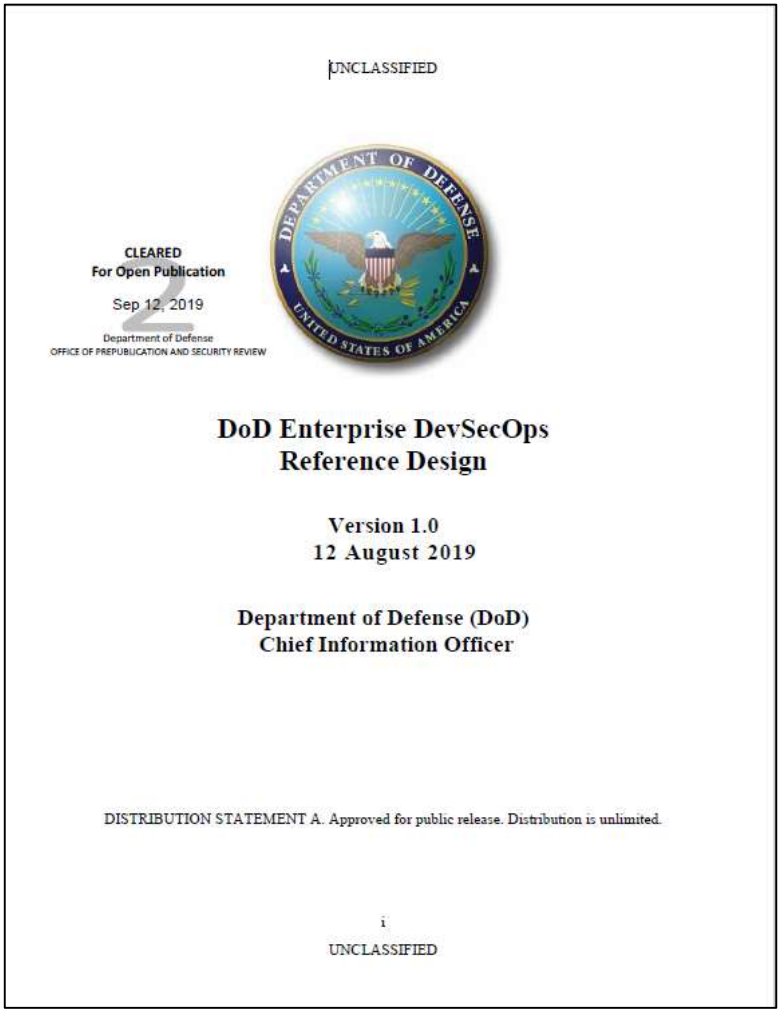
- Rate of change is disorienting decision makers
  - Growth curves go from linear to exponential to logarithmic
- Metric Categories are Important
  - Education, innovation, trade, economic and social outcomes
- Measurability
  - In the context of time
  - Quantified and Qualified variables
- Risk Indexing
  - Addressing the dynamic nature of multiple variables over time and in snapshots of time



DEVSECOPS
(Software Lifecycle)

- **DevSecOps**
  - An organizational software engineering culture and practice
  - Unifies software development (Dev), security (Sec) and operations (Ops).

- Main characteristics
  - ***Automate***, monitor, and apply security at all phases of the software lifecycle: plan, develop, build, test, release, deliver, deploy, operate, and monitor.
  - Automated unit, functional, integration, and security testing
  - Security and functional capabilities are tested and built simultaneously.



UNCLASSIFIED

CLEARED
For Open Publication
Sep 12, 2019
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DoD Enterprise DevSecOps Reference Design

Version 1.0
12 August 2019

Department of Defense (DoD)
Chief Information Officer

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

i

UNCLASSIFIED

12Aug2019

Metrics and Desired Outcomes

- Reduced mean-time to production: the average time it takes from when new software features are required until they are running in production
- Increased deployment frequency: how often a new release can be deployed into the production environment
- Fully automated risk characterization, monitoring, and mitigation across the application lifecycle
- Software updates and patching at "the speed of operations".

New Mandates
2020

- **Defense Industrial Base:**
  - The aggregate loss of controlled unclassified information (CUI) from the DIB sector increases risk to national economic security and in turn, national security. In order to reduce this risk, the DIB sector must enhance its protection of CUI in its networks.

- **Cybersecurity Maturity Model Certification**
  - DOD is planning to migrate to the new CMMC framework in order to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB).
  - The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene as well as protect controlled unclassified information (CUI) that resides on the Department's industry partners' networks.

Implications for Innovation:

- Barrier to entry for Small Biz
- Third Party Certification required
- CMMC still immature
- Third Party Certifier not yet designated
- Mandatory Level 3+ to be part of DIB