Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 31
Issue 3 *01/01/2015*

Article 1

January 2014

# Long on Rhetoric, Short on Results: Agile Methods and Cyber Acquisitions in the Department of Defense

Daniel E. Schoeni USAF

# LONG ON RHETORIC, SHORT ON RESULTS: AGILE METHODS AND CYBER ACQUISITIONS IN THE DEPARTMENT OF DEFENSE

**Major Daniel E. Schoeni, USAF**†

*What is of the greatest importance in war is speed.*[1]
— Sun Tzu

*Amateurs talk about tactics, but professionals study logistics.*[2]
— General Robert H. Barrow, USMC

TABLE OF CONTENTS

INTRODUCTION .....386
I. BACKGROUND .....387
A. Hackers, Cyberattacks, and the Need for Cybersecurity .....388
B. Cyberattacks on the DoD and National Security. .....391
C. The DoD and Cyber Acquisitions .....393
D. Three Qualifications .....396
II. THE AGILE SOFTWARE DEVELOPMENT METHOD .....398
A. Pre-Agile Software Development Methods .....398
B. The Agile Method of Software Development .....402
C. Agile's Proven Success .....404
III. THE HISTORY OF FEDERAL SOFTWARE PROCUREMENT AND DEVELOPMENT .....405

---

† Major Schoeni is a graduate of Brigham Young University (B.A.), the University of Iowa (J.D./M.A. Philosophy), the University of Nottingham (LL.M.), and most recently George Washington University (LL.M.). He has been on active duty since 2004, and is currently assigned as program counsel at Hanscom AFB, Massachusetts. An earlier version of this paper was submitted for Professor Paul Rosenzweig's cybersecurity seminar. Special thanks go to Professors Rosenzweig and Daniel I. Gordon of George Washington University, as well as Mr. Ronald I. Lee of Arnold & Porter, LLP, for their helpful comments. The views expressed here are the author's and do not reflect an official position of the Department of the Air Force, Department of Defense, or any other U.S. government agency.

1. SUN TZU, THE ART OF WAR 69–70 (1963).
2. PHILIP FROHNE, QUANTITATIVE MEASUREMENTS FOR LOGISTICS 107 (2007).

A. An Overview of IT Procurement Policy Since the 1960s .....406
B. The Federal Government's Experience with Iterative, Waterfall, and Agile Software Development Methods.....406
IV. PROBLEMS WITH ADOPTING AGILE IN THE DOD AND HOW TO FIX THEM.....412
A. DoD Software Development Still Resembles The Waterfall Method.....412
B. Federal Law or Regulations Do Not Preclude Agile; Instead, Culture and Bureaucratic Inertia Impede Change.....415
C. To the Extent That Federal Procurement Law and Regulations Are To Blame, There Are Several Reforms That May Help.....418
CONCLUSION .....423

## INTRODUCTION

Cyber warfare has arrived. The Department of Defense (DoD) is under attack, and our security is at stake. Yet in a field defined by its rapid growth, the DoD arms itself at the same pace that that it buys major weapons systems, an acquisition cycle of 7–10 years. It thus buys obsolete cyber-defense tools. The "arsenal of democracy"[3] has already provided us the tools for overcoming this impediment in the form of agile software-development methods. Yet the DoD has been reluctant to set aside decades of experience and utilize different methods for software than it does for other acquisitions. But unless it does so, it may well lose its edge, and not only in the cyber domain.

The next four sections will proceed as follows. The first describes the growing threat of cyberattacks generally, discusses how they affect the DoD and our security specifically, and then explains the relationship between DoD cybersecurity and rapid-cyber procurement.[4] The second summarizes agile software development—

3. Though it was FDR who made this phrase famous in his eponymous speech on December 29, 1940, it was industrialist Bill Knudson who coined the term. After a successful career at Ford and GM, Knudson was chosen to head up the National Defense Advisory Council, the group charged with retooling America's peacetime economy for war. *See* ARTHUR HERMAN, FREEDOM'S FORGE: HOW AMERICAN BUSINESS PRODUCED VICTORY DURING WW II 69–71, 115, 129 (2012).

4. This paper is not the first to suggest the connection between cybersecurity and acquisition practices. In fact, on January 23, 2014, Secretary of Defense Chuck Hagel and Daniel M. Tangherlini of the General Services Administration wrote a memorandum to the assistants to

its history, methods, and track record. The third recounts the history of federal and DoD IT acquisitions and the DoD's attempt at agile reforms. Though underway for a decade or more, there is little to show for it. The last section focuses on the analysis of why agile has not taken root, how to foster such reforms in the DoD, and benefits that may accrue.

## I. BACKGROUND

This section first considers cyberspace dangers generally, then the unique threat to the DoD, and finally problems with its acquisitions practices. After discussing these dangers and the DoD's unpreparedness in this domain, the next section turns to the agile method as alternative to the current software-development model.

To avoid any confusion, it bears mentioning that this paper uses the terms *cyber*, *software*, and *information technology* (IT) almost interchangeably—the first as an adjective, and the latter two as nouns for the same concept. Although both the introduction and background that follows concentrate on cybersecurity, concerns about software development and acquisition practices apply more broadly. Because the DoD relies on software for more than cyberattack and defense,[5] its acquisition practices are of wider concern. Thus, while there are admittedly differences between cyber, software, and IT,[6] they are related terms and this paper will not dwell on their distinctions.

---

the president for homeland security and economic affairs forwarding a study on this subject. IMPROVING CYBERSECURITY AND RESILIENCE THROUGH ACQUISITION: FINAL REPORT OF THE DEPARTMENT OF DEFENSE AND GENERAL SERVICES ADMINISTRATION, S.C493D22 (2013).

5. *See infra* note 25.

6. The OXFORD ENGLISH DICTIONARY ONLINE reports that "cyber" is an adjective that first came into use in 1992 meaning "of, relating to, or involving (the culture of) computers, virtual reality, and or the Internet." *Cyber Definition*, OXFORD ENG. DICTIONARY ONLINE, http://www.oed.com.proxygw.wrlc.org/view/Entry/250878?rskey=V6b5Z3&result=1#eid (last visited Mar. 3, 2014). It reports that "information technology" is a noun and relatively older term coming into use in 1952 referring to the "branch of technology concerned with the dissemination, processing, and storage of information, esp. by means of computers." *Information Technology Definition*, OXFORD ENG. DICTIONARY ONLINE, http://www.oed.com.proxygw.wrlc.org/view/Entry/273052?redirectedFrom=information+technology#eid (last visited Mar. 3, 2014). And it reports that "software" came into use almost a decade later (1960) and signifies the "programs and procedures required to enable a computer to perform a specific task, as opposed to the physical components of the system." *Software Definition*, OXFORD ENG. DICTIONARY ONLINE, http://www.oed.com.proxygw.wrlc.org/view/Entry/183938?redirectedFrom=software#eid (last visited Mar. 3, 2014). There are some obvious distinctions among the terms. For example, IT and software have overlapping but not coextensive definitions; the former encompasses not only software but also hardware, the latter only software. Further, the Federal Acquisition Regulation (FAR) has its own definitions for these terms that differ in some respects from the common usage. *See, e.g.*, FAR 2.101 (making a distinction between the term "computer software," which means, "programs

### *A. Hackers, Cyberattacks, and the Need for Cybersecurity*

The fight for security, in both private and public sectors, is part of what Michael Gross calls "World War 3.0" in his eponymous *Vanity Fair* article.[7] He explains that the Web's openness makes users vulnerable to "various kinds of hacking, including corporate and government espionage, personal surveillance, the hijacking of Web traffic, and remote manipulation of computer-controlled military and industrial processes."[8]

Consistent with Gross's account, reports of cybercrime,[9] large companies being hacked,[10] and cyberattacks on government agencies[11]

---

that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations" and the term "computer data bases"); *see also* JAMES G. MCEWEN, DAVID S. BLOCH, RICHARD M. GRAY & JOHN T. LUCAS, INTELLECTUAL PROPERTY IN GOVERNMENT CONTRACTS: PROTECTING AND ENFORCING IP AT THE STATE AND FEDERAL LEVEL 76–83 (2d ed. 2012) (explaining the definitions of computer software and related terms under the FAR and DFARS).

7. Michael Gross, *World War 3.0*, VANITY FAIR (May 2012), http://www.vanityfair.com/news/2012/05/internet-regulation-war-sopa-pipa-defcon-hacking.

8. *Id.*

9. *See, e.g.*, Elizabeth A. Harris et al., *Sneaky Path Into Target Customers' Wallets*, N.Y. TIMES, Jan. 18, 2014, at A1 (describing Eastern European hackers' $18 billion theft from consumers using debit cards at Target); *The Digital Arms Trade*, ECONOMIST (Mar. 30, 2013), http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade/ (describing the market of selling software "exploits" to organized crime and terror groups); Richard A. Clarke, *Stop Ignoring Online Thieves*, WASH. POST, Feb. 8, 2013, at A17 (claiming cybercrime is a multi-billion dollar industry); Misha Glenny, MCMAFIA: A JOURNEY THROUGH THE GLOBAL CRIMINAL UNDERWORLD 264–86 (2008) (detailing Brazilian mafia's cybercrime connections with Russia).

10. *See, e.g.*, Hayley Tsukayama, *Apple Hit by Hackers who Attacked Facebook*, WASH. POST, Feb. 20, 2013, at A12 (explaining that hackers attacked both companies exploiting a backdoor in Oracle's Java program to insert malware); Nicole Perlroth, *American Banks' Sites Are Attacked By Hackers*, N.Y. TIMES Jan. 5, 2013, at B2 (describing attacks on Bank of America, Citigroup, U.S. Bank, Wells Fargo, and PNC by al-Qassam group "in retaliation for an anti-Islam video"); David E. Sanger & Nicole Perlroth, *Cyberattacks on the Rise Against U.S. Corporations*, N.Y. TIMES, May 13, 2013, at A6 (warning of new attacks against businesses coming from the Middle East seeking to interfere with industrial machinery); *U.S.-China Economic and Security Review Commission Report*, CQ CONGRESSIONAL TESTIMONY, Nov. 20, 2013 (citing U.S. Cyber Command estimate that U.S. companies lose $250 billion annually to espionage); Nathaniel Popper, *Wall Street's Exposure To Hacking Laid Bare*, N.Y. TIMES, July 26, 2013, at B1 (detailing indictment of two hackers who gained access to NASDAQ for two years); *see also* Danny Palmer, *A Third of SMBs Unaware They've Been Cyber Attack Victims*, COMPUTING (Nov. 19, 2013), http://www.computing.co.uk/ctg/news/2307942/a-third-of-smbs-unaware-theyve-been-cyber-attack-victims (reporting that small businesses are under attack, but often lack the resources to know it); CLINT WITCHALLS, ECONOMIST INTELLIGENCE UNIT, INFORMATION RISK: MANAGING DIGITAL ASSETS IN A NEW TECHNOLOGY LANDSCAPE 10 (James Chambers ed., 2013), *available at* http://www.economistinsights.com/technology-innovation/analysis/information-risk (reporting that small businesses are sometimes special targets of cyberattacks).

11. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-09-661T, CYBER THREATS AND VULNERABILITIES PLACE FEDERAL SYSTEMS AT RISK (2009) (summary of Congressional

have become so common that they barely register.[12] Yet, though we may be inured, our networks are not, and our economy and way of life have come to depend on the Internet.

These threats come from a variety of sources including state actors, organized crime, and assorted anarchists. At present, state actors are most sophisticated,[13] with organized crime close at heel.[14] Yet while anarchist groups' skills were once modest, or at least not widely

---

testimony); *Australia Police, Central Bank Websites Hacked*, PHYS ORG (Nov. 21, 2013), http://phys.org/news/2013-11-australia-police-central-bank-websites.html; Steven Stalinsky, *China Isn't the Only Source of Cyberattacks,* WALL ST. J., May 22, 2013, at A17 (reporting that Tunisian Cyber Army and al-Qaeda Electronic Army hacked the DoD, State Department, and Department of Homeland Security); William Wan & Ellen Nakashima, *Chinese Cyberspying Hits More Than 140 Targets, Report Says*, WASH. POST, Feb. 20, 2013, at A08 (citing Mandiant report indicating that a dozen agencies had been infiltrated); Lisa Rein, *Virus Infects Computers at Commerce Dept. Agency*, WASH. POST (Feb. 3, 2012), http://www.washingtonpost.com/politics /commerce-agencys-system-infected-by-virus-may-be-victim-of-cyber-attack/2012/02/02/gIQA ViHWlQ_story.html (describing attack that forced the Department of Commerce to shut down internet access for 10 days); Paul Elias, *Federal Agencies Pursue Anonymous*, WASH. POST, Sep. 12, 2011, at A23 (reporting that LulzSec, an Anonymous affiliate, hacked the CIA's website); William J. Lynn III, *Defending a New Domain Subtitle: The Pentagon's Cyberstrategy*, 89 FOREIGN AFF. 97 (2010) (confirming a successfully attack on U.S. Central Command in 2008 using infected flash drives, previous reports suggested Russia was to blame); John Markoff, *China Link Suspected In Hacking Of Arms LabFolder*, N.Y. TIMES, Dec. 9, 2007, at A40 (reporting that the Chinese hacked into the Oak Ridge National Laboratory in Tennessee where nuclear weapons research is conducted). Moreover, this threat not only affects the federal government, but also affects states and local government. *See, e.g.*, John Stephenson & Karla Jones, *Fighting Cyber Warfare at the State Level*, WALL ST. J., Feb. 23, 2013, at A11 (describing numerous threats including "hackers breaking into power grids, communications networks and other critical systems, wreaking havoc by rendering these systems useless during an emergency").

12. Common as reports are, they likely underreport the frequency of attacks. Businesses are secretive about when they have been hacked as "publishing specific details about hacks will highlight weak spots, or at least point to where most attention or resources are being deployed," and "even talking about cyber-attacks can attract more attention from cyber-attackers." James Chambers, *Cracking the Code of Silence*, ECONOMIST INTELLIGENCE UNIT (Nov. 20, 2013), http://www.economistinsights.com/technology-innovation/opinion/code-silence.

13. *See, e.g.*, BRANDON VALERIANO & RYAN C. MANESS, CYBER WAR VERSUS CYBER REALITIES: CYBER CONFLICT IN THE INTERNATIONAL SYSTEM 25 (2015) (explaining that large state actors "seem to be the most dominant cyber actors because they have the resources, manpower, and money to support massive cyber operations").

14. *See, e.g.*, Caroline Fairchild, *Target Security Breach Likely to Be 'Highly Sophisticated Organized Crime,'* FORTUNE (Dec. 13, 2013), http://fortune.com/2013/12/19/tar get-security -breach-likely-to-be-highly-sophisticated-organized-crime/ (reporting that organized crime's hacking skills are increasingly sophisticated); Steve Ranger, *Organized Cybercrime Groups Are now as Powerful as Nations*, ZDNET, Jun. 9, 2014, http://www.zdnet.com/article/organised-cyber crime-groups-are-now-as-powerful-as-nations/ (describing the proliferation of cybercrime as "hackers share skills to build complex attacks to steal cash and intellectual property"); *Cyber Security: Protecting America's New Frontier*, *Hearing Before the Subcomm. on Crime, Terrorism & Homeland Security*, 121st Cong. 5 (2011) (warning that "cyber crime on the rise with criminal syndicates operating with increasing sophistication").

distributed among their ranks,[15] their sophistication increases daily and poses a growing cause for concern.[16]

Perhaps the best indicator of how serious all of this has become is that government is not alone in the effort to steel itself against the growing threat.[17] The private sector has likewise taken notice. Cybersecurity has become a multi-billion dollar industry.[18] Firms have started buying cyber insurance.[19] And some advocate for their right to "hack back" when they are attacked.[20] Some commentators argue the private sector nevertheless underestimates the dangers and spends less than it should on cyber self-defense.[21] In any event, the private sector's growing awareness of, and efforts to protect itself from, cyberattacks suggest that cybersecurity risks are as ubiquitous as they are real.[22]

---

15. *See* PARMY OLSON, WE ARE ANONYMOUS 36–37, 80 (2012) (describing methods of early attacks by Anonymous members as effective yet technically unsophisticated and their evolution since then).

16. *See* Jim Finkle & Joseph Minn, *Exclusive: FBI Warns of U.S. Government Breaches by Anonymous Hackers*, REUTERS (Nov. 15, 2013), http://www.reuters.com/article/2013/11/15/us-usa-security-anonymous-fbi-idUSBRE9AE17C20131115 (giving Anonymous credit for exploiting flaws in Adobe software to hack into "U.S. Army, Department of Energy, Department of Health and Human Services, and perhaps many more agencies").

17. *See, e.g.*, Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11739 (Feb. 12, 2013) (explaining that the "cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges").

18. Press Release, Gartner Says Worldwide Security Market to Grow 8.7 Percent in 2013, (June 11, 2013), http://www.gartner.com/newsroom/id/2512215 (announcing that cybersecurity would reach an estimated $67.2 billion in 2013 and projecting $86 billion in 2016); *see also* ECONOMIST, *Cyber-Security: White Hats To The Rescue*, Feb. 22, 2014, at 55–56 (describing a growing market for "white hat" hackers to do penetration tests to identify cybersecurity weaknesses).

19. *See* James Willhite, *On Alert Against Cybercrime—More CFOs Weigh Insurance Against Data Breaches, Despite Limits on Coverage*, WALL ST. J., Aug. 13, 2013, at B6 (citing a survey showing that 31% of firms buy business insurance largely due to cybersecurity threats). *But see* STEPHEN E. FLYNN & DANIEL B. PRIETO, COUNCIL ON FOREIGN RELATIONS, CSR NO. 13, NEGLECTED DEFENSE: MOBILIZING THE PRIVATE SECTOR TO SUPPORT HOMELAND SECURITY 23–24 (2006), *available at* http://www.cfr.org/border-and-port-security/neglected-defense/p10457 (arguing that cybersecurity insurance won't take off without government engagement).

20. Christopher M. Matthews, *Cybertheft Victims Itchy to Retaliate*, WALL ST. J., June 3, 2013, at B6 (describing the business community's growing support for responding to hackers in kind)); James Podgers, *Should Hacked Firms Be Cybercops?*, A.B.A. J. (Apr. 1, 2013), http://www.abajournal.com/magazine/article/should_hacked_firms_be_cybercops/ (recounting a panel on active cyber defense and referencing ABA's ongoing work in this area); PAUL ROSENZWEIG, CYBER WARFARE: HOW CONFLICTS IN CYBERSPACE ARE CHALLENGING AMERICA AND CHANGING THE WORLD 69 (2013) (noting the possibility of issuing letters of marque and reprisal to private companies under the U.S. CONST., art. 1, § 8, cl. 11).

21. *See, e.g.*, *id.* 157–65 (providing an economic rationale for the private market's underspending on cybersecurity given the high level of threat posed).

22. One need look no farther than one's own wallet to see evidence of the private sector's growing efforts to protect consumers from mounting cybersecurity threats. Following last year's

*B. Cyberattacks on the DoD and National Security.*

Far from being immune to the increasing risks just described, the DoD faces even greater cyber threats because it is such an attractive target.[23] That is not only due to its dominance, but also because it is so dependent on IT.[24] To illustrate, 90% of weapons systems' functionality relies on software.[25] So cyber warfare tempts our "adversaries because it poses a significant risk at low cost."[26] Indeed, such adversaries scan DoD networks millions of times a day searching for weaknesses, and weaknesses they have found, thereby pilfering blueprints to some of our most advanced weapons.[27] This is no longer the stuff of science fiction or far-fetched airport spy thrillers. High-stakes cyber espionage has arrived.

The DoD recognizes the threats, and has instituted plans for preventing, defending from, and mitigating them.[28] It has also taken some steps to shore up the security of the industrial base,[29] which not only houses state-of-the-art weapons designs but has proven quite

attack on Target, *see* Harris et al., *supra* note 9, U.S. banks have announced they will adopt cards with embedded chips affording better security. Joe Nocera, *Dogged by Data Theft*, N.Y. TIMES, Feb. 11, 2014, at A27 (describing the efforts to adopt the European-style "chip-and-PIN" card that both "encrypts data and authenticates the card").

23. DAVI D'AGOSTINO & GREG WILSHUSEN, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-75, DEFENSE DEPARTMENT CYBER EFFORTS: DOD FACES CHALLENGES IN ITS CYBER ACTIVITIES 1–2 (2011).

24. *Id.* (noting that although the DoD operates 7 million computers and 10,000 networks it failed to appreciate the danger until its inept response to a malware attack in 2008 "exposed the weakness of the DoD's command and control authorities . . . for cyberspace operations").

25. REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON DEPARTMENT OF DEFENSE POLICIES AND PROCEDURES FOR THE ACQUISITION OF INFORMATION TECHNOLOGY 6 (2009) (explaining that software accounted for only 20% of weapons' functionality in 1970, increased to 80% in 2000, and now accounts for 90%) (citing DEFENSE SCIENCE BOARD TASK FORCE ON DEFENSE SOFTWARE (2000); PROGRAM MANAGER'S GUIDE FOR MANAGING SOFTWARE (2001)); *see also* NATIONAL RESEARCH COUNCIL, CRITICAL CODE: SOFTWARE PRODUCIBILITY FOR THE DEPARTMENT OF DEFENSE 17–19 (2010) (explaining that software "is increasingly used to embody the functionality of defense systems of all kinds" and "at the core of the ability to achieve integration and maintain agility" of the use of technology as "force multiplier"); Barry Boehm, Richard Turner, & Peter Kind, *Risky Business: Seven Myths About Software Engineering That Impact Defense Acquisitions*, 31 PROGRAM MANAGER (2002) (quoting an Air Force General saying, "About the only thing you can do with an F-22 without software is take a picture of it.").

26. D'AGOSTINO & WILSHUSEN, *supra* note 23, at 1–2.

27. *Id.*

28. *See* QUADRENNIAL DEFENSE REVIEW 37–39 (2010) ("Operating Successfully in Cyberspace").

29. *See, e.g.*, Defense Federal Acquisition Regulation Supplement (DFARS) Safeguarding Unclassified Controlled Technical Information, 78 Fed. Reg. 69273 (final rule issued Nov. 18, 2013) (to be codified at 48 C.F.R. parts 204, 212, 252) (adding DFARS clause requiring defense contractors to report to the DoD when sensitive information has been compromised, e.g., cyber espionage).

vulnerable to espionage.[30] One expert testified that the Chinese have stolen plans for the F-35 from Lockheed-Martin, Northrop-Grumman, and BAE,[31] and another 50 weapons systems, including Patriot and Aegis missile defense systems, V-22 Osprey, F/A-18 fighter, and Littoral Combat Ship have also been stolen.[32] That is to list only examples of espionage, while the DoD faces a wider range of threats.[33] Collectively, "such threats," James Clapper, the Director of National Intelligence, has said, "pose a critical national and economic security concern."[34] Federal acquisition policy and practice play an important role in addressing these threats.[35]

30. *See, e.g.*, MANDIANT, APT1: EXPOSING THE THREAT OF ONE OF CHINA'S CYBER ESPIONAGE UNITS (2012) (uncovering cyber espionage against 151 U.S. companies committed over seven years); Danny Yadron, *Chinese Hacked U.S. Military Contractors*, WALL ST. J. ONLINE (Sept. 18, 2014), http://online.wsj.com/articles/chinese-hacked-u-s-military-contractors-senate-panel-says1410968094?mod=WSJ_hps_sections_news (writing that Chinese hackers have broken into computer networks of private transportation companies working for the U.S. military 20 times in the past year); *see also* DFARS Safeguarding Unclassified Controlled Technical Information, 78 Fed. Reg. 69273 (Nov. 18, 2013) (codified as 48 C.F.R. Parts 204, 212, 252) (adding clause to safeguard information held by defense contractors).

31. CYBER ESPIONAGE AND THE THEFT OF U.S. INTELLECTUAL PROPERTY AND TECHNOLOGY (2013) (testimony of Dr. Larry M. Wortzel, Strategic Studies Institute), http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf.

32. *Id.* (citing Ellen Nakashima, *Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies*, WASH. POST (May 27, 2013), http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html).

33. For example, fighter jets make attractive targets for hackers because of "their reliance on software and information technology," and controlling the software is to control the hardware. *See* Brendan McGarry, *Is the F-35's Computer R2-D2 or HAL?*, DEFENSETECH (Feb. 19, 2014), http://defensetech.org/2014/02/19/is-the-f-35s-computer-r2-d2-or-hal/ (citing David Martin, *Is the F-35 Worth It?*, 60 MINUTES (Feb. 15, 2014), http://www.cbsnews.com/news/f-35-joint-strike-fighter-60-minutes/; *Can the U.S. Military's New Jet Fighter Be Hacked?*, 60 MINUTES OVERTIME (Feb. 16, 2014), http://www.cbsnews.com/news/can-the-f-35-be-hacked/ (describing the risk of cyberattacks on "ALIS," the F-35 fighter jet's onboard computer). The author is indebted to Steven Schooner for alerting him of this report.

34. GREGORY C. WILHUSEN, U.S. GOV'T ACCOUNTABILITY OFFICE GAO-12-666T, CYBERSECURITY: THREATS IMPACTING THE NATION 1 (2012) (summary of Congressional testimony) (citing JAMES L. CLAPPER, UNCLASSIFIED STATEMENT FOR THE RECORD ON THE WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY FOR THE SENATE SELECT COMMITTEE ON INTELLIGENCE (2012)).

35. *See* IMPROVING CYBERSECURITY AND RESILIENCE THROUGH ACQUISITION, *supra* note 4 (making recommendations to the president on the "feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration").

### *C. The DoD and Cyber Acquisitions*

In 1965, Intel's founder Gordon Moore famously predicted that computer processing power would double every year,[36] later revising that prediction to two years.[37] His prediction has held true for the last five decades, and we have seen exponential growth rates in various measures of technological growth, including processing speed, memory capacity, and digital camera pixels.[38] Such rapid growth is significant for our increasingly cyber-dependent military, which relies not only on instantaneous worldwide communication but also on military hardware whose functionality heavily depends on software.[39] "In short," wrote the Defense Science Board, "more software, means more vulnerability."[40]

This weakness is not lost on our adversaries.[41] It is compounded by the DoD's longstanding problem with slow IT acquisition, which the Obama-Biden transition team in 2009 aptly called "fundamentally broken."[42] While cyberattacks happen in mere seconds,[43] IT acquisition is measured in months and years.[44] With a few exceptions discussed later, the DoD purchases software like major weapons systems,[45] and

---

36. *See* Gordon E. Moore, *Cramming More Components onto Integrated Circuits*, 38 ELECTRONICS MAG. (Apr. 19, 1965).

37. *See* Gordon E. Moore, *Progress in Digital Integrated Electronics*, 21 IEDM TECH. DIGEST 11, 11–13 (1975), *available at* http://www.lithoguru.com/scientist/CHE323/Moore 1975.pdf.

38. NAT'L RESEARCH COUNCIL, MEASURING AND SUSTAINING THE NEW ECONOMY: ENHANCING PRODUCTIVITY GROWTH IN THE INFORMATION AGE 6 (Dale W. Jorgenson & Charles W. Wessner eds., 2006). Though "processing speed is no longer increasing at this rate," DEFENSE SCIENCE BOARD REPORT *supra* note 25 at 7, quantum computers may soon overcome this barrier. *See, e.g.*, Quentin Hardy, *A Big Leap To Quantum Computing*, N.Y. TIMES, May 11, 2013, at B11.

39. DEFENSE SCIENCE BOARD REPORT, *supra* note 25, at 6 (explaining software currently provides 90% or more of a weapon's system's functionality).

40. *Id.* at 17.

41. *See id.*

42. NATIONAL RESEARCH COUNCIL, ACHIEVING EFFECTIVE ACQUISITION OF INFORMATION TECHNOLOGY IN THE DEPARTMENT OF DEFENSE 28–29 (2010).

43. *Id.* at 23 (explaining that "cyber attacks on IT systems used to be lengthy, planned-out attacks, but now automated scanning, analysis, and global sharing of attack vectors enable attack cycles to occur in minutes and sometimes seconds").

44. *Id.* (explaining the "overall portfolio of DOD IT programs has experienced a 21-month delay in delivering initial operational capability to the war fighter, and 14 percent are more than four years late") (citing KATHERINE V. SCHINASI, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-782T, DEFENSE ACQUISITIONS: BETTER WEAPON PROGRAM OUTCOMES REQUIRE DISCIPLINE, ACCOUNTABILITY, AND FUNDAMENTAL CHANGES IN THE ACQUISITION ENVIRONMENT 5 (2008) (Congressional testimony)).

45. Many have argued that the process does not work well for major weapons systems either. *See, e.g.*, Secretary Robert M. Gates, *A Balanced Strategy: Reprogramming the Pentagon for a New Age*, FOREIGN AFF. (May/June 2009) (arguing that the Pentagon's acquisition system

this is a process that can take 7–10 years from planning to delivery.[46] That the rest of the government has similar problems is of only small consolation,[47] as these are not only life and death matters for the individual warfighter, but also bear on our military readiness and national security more generally. In short, defending from cyberattacks and developing state-of-the-art cyber weapons depend on acquisition that moves on par with the pace of technological growth. Though the DoD far outspends its strategic rivals,[48] volume will be to no avail if its weapons are already obsolete when fielded.[49] And as important as superior technology can be to warfare,[50] it can be fleeting[51]—all the more so if our acquisitions move at a much slower pace than that at which technology changes.

---

is "baroque" and that deployed warfighters need solutions that can be fielded in months and weeks rather than in years); MICHAEL J. SULLIVAN, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-1159T, DEFENSE ACQUISITIONS: FUNDAMENTAL CHANGES ARE NEEDED TO IMPROVE WEAPON PROGRAM OUTCOMES 1–3 (2008) (testifying that "continue to take longer, cost more, and deliver fewer quantities and capabilities than originally planned" despite GAO warnings since 1990).

46. Colin Clark, *Army Cyber Chief Meets Buyers In Pursuit Of Faster Acquisition*, BREAKING DEFENSE (Oct. 22, 2013), http://breakingdefense.com/2013/10/army-cyber-chief-meets-buyers-in-pursuit-of-faster-acquisition/.

47. *See, e.g.*, Clay Johnson & Harper Reed, Op-Ed, *Why the Government Never Gets Tech Right*, N.Y. TIMES, Oct. 25, 2013, *available at* http://nyti.ms/1DWmXtK (reporting that in the last 10 years more than half of all large federal IT programs have been delayed and 41% have failed users' expectations); Katherine M. John, *Information Technology Procurement in the United States and Canada: Reflecting on the Past with an Eye Toward the Future*, 48 PROCUREMENT LAWYER 4, 5 (2013) (noting "a recurrent criticism of federal government IT is that it fails to keep pace with private sector advancements"); Steven Brill, *Code Red*, TIME, Mar. 10, 2014, at 26 (recounting the story of the private sector experts who rescued the HealthCare.gov Website).

48. *See, e.g.*, THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES, THE MILITARY BALANCE 548–54 (2013) (providing tables illustrating that the United States' disproportionate defense spending compared with other nations); David Wessel, *Everything You Ever Wanted To Know About The Budget But Were Afraid to Ask*, WALL ST. J., Jul. 12, 2012, at C3 (reporting that the "U.S. defense budget is greater than the combined defense budgets of the next 17 largest spenders").

49. Further, money cannot buy timely software delivery. Counterintuitively, Brooks's Law says assigning more manpower to a troubled software project can actually slow down development. *See* FRED BROOKS, THE MYTHICAL MAN MONTH: ESSAYS ON SOFTWARE ENGINEERING 25, 274 (1975).

50. *See infra* note 56 (describing the distinct advantages of superior technology in warfare).

51. P.W. SINGER, WIRED FOR WAR: THE ROBOTICS REVOLUTION AND CONFLICT IN THE 21ST CENTURY 238–41 (2009) (warning about the risk of complacency about superior American technology).

Military and political leaders recognize that this must change.[52] Several studies have reached this conclusion,[53] and the Defense Science Board warned:

> The deliberate process through which weapon systems and information technology are acquired by DOD cannot keep pace with the speed at which new capabilities are being introduced in today's information age—and the speed with which potential adversaries can procure, adapt, and employ those same capabilities against the United States.[54]

The DoD recently concluded that rapid IT-acquisition processes are "vital to national security" and is adjusting its policies and strategies accordingly.[55] Later sections will consider how effective those efforts have been, explain why they have largely failed to deliver, and offer

---

52. *See, e.g.*, Clark, *supra* note 46 (Army's top cyber commander saying "he wanted to buy 'faster, better, quicker' since the cyber realm doesn't really allow for the seven to 10 years a standard acquisition program usually takes."); Ellen Nakashima, *Pentagon to Fast-Track Cyberweapons Acquisition*, WASH. POST, Apr. 10, 2012, at A3 (reporting that Pentagon officials recognize that sometimes "risk to operations and personnel" caused by slow cyber acquisitions "is unacceptable"); Amber Corin, *Navy: Faster Acquisition Key to Cyber Defense*, FCW (June 28, 2011), http://fcw.com/articles/2011/06/28/cyber-warfare-summit-acquisition-reform-strategies.aspx (reporting that "existing acquisition model . . . is ill-equipped to meet the fast-moving needs of cyber defense"); Bob Brewin, *Air Force Cyber Chief: Speed Up Acquisitions Already*, NEXTGOV (Feb. 8, 2012), http://www.nextgov.com/defense/2012/02/air-force-cyber-chief-speed-up-acquisitions-already/50600/ (Air Force Space Command's top general lamenting that DoD "acquires cyber capabilities the same way it buys aircraft or satellites," which "can take years, while new developments in computer hardware and software can happen in days or months"); Rex B. Reagan & David F. Rico, *Lean and Agile Acquisition and Systems Engineering: A Paradigm Whose Time Has Come*, DEF. AT&L, Nov.–Dec. 2010, at 48, 52 (quoting General David H. Petraeus who called for "adaptive, responsive, and speedy acquisitions" because our enemies are "unlike any enemy fought in the past, demonstrating different tactics, techniques, and procedures from those found in conventional warfare").

53. *See, e.g.*, ISAAC R. PORCHE III ET AL., RAPID ACQUISITION & FIELDING FOR INFORMATION ASSURANCE & CYBER SECURITY IN THE NAVY iii (2013) (explaining that "today's acquisition approach is not geared toward cyber security," that we need "a cyber acquisition process that can react much faster than formal [DoD] channels, and that "the primary reason for this need is that many cyber technologies and products have fast development and deployment cycles that must be matched with rapid acquisition processes to avoid obsolescence when deployed"); MARY ANN LAPHAM ET AL., AGILE METHODS: SELECTED DOD MANAGEMENT AND ACQUISITION CONCERNS 2–3 (Carnegie Mellon Software Eng'g Inst., 2011) (describing need for "acquisition tempos that respond to operational tempos" and that the warfighter is endangered if he doesn't have what he needs when he needs it); CARLTON NORTHERN ET AL., MITRE CORP., HANDBOOK FOR IMPLEMENTING AGILE IN DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY ACQUISITION (2010) (holding that "heavyweight" processes for major weapons are ill-suited to IT because when "finally fielded, the technology is dated and the functionality needed 5 to 10 years before may no longer address the Warfighter's current needs").

54. DEFENSE SCIENCE BOARD REPORT, *supra* note 25, at 1.

55. DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 10 (2011), *available at* www.defense.gov/news/d20110714cyber.pdf

some ideas about the way forward. The DoD must figure out how to expedite the cyber-acquisition process. Before proceeding, however, three qualifications are in order.

### *D. Three Qualifications*

This paper does not maintain that the latest weaponry ensures success in the physical or cyber domains. Technical advantage is at most necessary;[56] alone, it is not sufficient.[57] But since the Battle of Thermopylae, historians and tacticians have noted that battles often go to the soldiers who are best equipped.[58] So it will be in cyberspace. Militaries with high-tech cyber defenses will sometimes fall prey to inferior low-tech foes. Yet that will be the exception. Other things being equal, superior technology will usually win.

Second, not all software that the DoD uses is bespoke. While weapons systems require ground-up development, much of the software the DoD uses is for more mundane purposes: payroll, human

56. Examples of lower-tech armies defeating higher-tech rivals are not unknown, such as the Afghans repelling the Soviets. Such examples, however, are usually limited to Fabian tactics or guerilla warfare. In pitched battle, better-equipped armies time and again have proven devastatingly lethal. VICTOR DAVIS HANSON, CARNAGE AND CULTURE: LANDMARK BATTLES AND THE RISE TO WESTERN POWER 12–13, 19–20, 119–120 (2001) (arguing that our scientific and cultural tradition have given Western militaries an edge for 3,000 years). Further, myth sometimes misinterprets martial success. For example, though folklore sometimes depicts the Battle of Little Bighorn as a triumph of Stone Age weapons over hubris and modern arms, some argue that Custer's famous defeat was due in part to the Sioux carrying repeating rifles and the 7th Cavalry carrying inferior single-shot carbines. *See, e.g.*, RICHARD ALLAN FOX, JR., ARCHEOLOGY, HISTORY, AND CUSTER'S LAST BATTLE: THE LITTLE BIG HORN REEXAMINED 77–79 (1993). Stories about scrappy underdogs sell more books and movie tickets, but in real life the overdogs usually win. Having state-of-the-art weaponry is not *always* decisive, but it usually is.

57. Sometimes technology's role is exaggerated. Blitzkrieg victories had less to do with superior German military technology than with superior tactics. The British invented the tank during World War I, and the French perfected it in the 1930s. Yet neither saw tanks as strategically important offensive weapons. The French preferred using tanks merely as support for infantry and artillery units. By contrast, Hitler's success lay with the innovation of utilizing his Panzer divisions for rapid mechanized infantry attacks. *See* MAX BOOT, WAR MADE NEW: TECHNOLOGY, WARFARE, & THE COURSE OF HISTORY, 1500 TO TODAY 212–27 (2006); *see also id.* at 9–11 (noting that while "the tools of war do matter," he discourages "technological determinism" and urges that we avoid both undervaluing and overvaluing the role of technology in military history).

58. *See* VICTOR DAVIS HANSON, THE WESTERN WAY OF WAR: INFANTRY BATTLE IN CLASSICAL GREECE 55–56 (2009) (contrasting Greek armaments with the Persians who "in warlike spirit and strength . . . were not inferior, but they were unprotected with armor") (quoting Herodotus 9.62.4)); Joseph Kleist, *The Battle of Thermopylae: Principles of War on the Ancient Battlefield*, 6 STUDIA ANTIQUA 75, 80–81 (2008) (attributing the Spartan's relative success despite being vastly outnumbered in part to superior arms); Victor Davis Hanson, *Hoplite Technology in Phalanx Battle*, *in* HOPLITES: THE CLASSICAL GREEK BATTLE EXPERIENCE 63–64 (Victor Davis Hanson ed., 1991) (describing the "unique advantages of the hoplite shield and butt-spike to contemporary, phalanx warfare"); F.E. ADCOCK, THE GREEK AND MACEDONIAN ART OF WAR (1957) (explaining the significance of armor and shield technology to classical Greek infantry).

resources, logistics, and the like. When such software is available in the private market, the federal government should purchase it under FAR Part 12 ("Acquisition of Commercial Items").[59] Buying commercial is less expensive and "provides immediate access to rapidly evolving technology."[60] Where possible, purchasing commercial is always best. Accordingly, the agile development methods advocated in this paper concern only the unique requirements that cannot be met with commercial purchases. Such unique requirements will always be a large segment of DoD outlays.[61]

Third, both government employees and government contractors write software for the military. Yet because uniformed members, civilians, and contractors are increasingly seamless in their duties,[62] especially in the DoD,[63] this paper will not attempt to distinguish between them.[64] Criticism of current methods and suggestions about how they may be improved apply equally to both groups.

---

59. FAR 12.101(a) (establishing the policy that federal agencies are to research "commercial" and "nondevelopmental items" to see if they meet government requirements).

60. IMPROVING CYBERSECURITY AND RESILIENCE THROUGH ACQUISITION, *supra* note 4, at 11.

61. Secretary of Defense William J. Perry is widely credited with the commercial revolution in defense procurement in 1990s. He recognized that DoD IT acquisition couldn't keep pace with commercial advances, and advocated purchasing from commercial sources whenever possible. *See, e.g.*, William Perry, *Defense Must Open the Commercial Door*, L.A. TIMES, Feb. 23, 1998, at 5 (advocating buying commercial and holding that the DoD "must give up its unique buying practices and employ best commercial practices"); JACQUES S. GANSLER & WILLIAM LUCYSHYN, COMMERCIAL-OFF-SHELF (COTS): DOING IT RIGHT 7–8, app. (2008) (relating the "seminal" role of the 1994 "Perry Memo" on reshaping acquisitions to buy from commercial sources, and including the memorandum in the appendix). The problem is that this can go only so far. Much of what the military buys is truly unique and isn't available commercially.

62. *See* Sondra Bell Nensala, *Homeland Security Presidential Directive 12: How HSPD-12 May Limit Competition Unnecessarily and Suggestions for Reform*, 40 PUB. CONT. L.J. 619, 661–62 (2011) (describing the government's 251% increase in the outsourcing of IT during the 1990s); Dan Guttman, *Governance by Contract: Constitutional Visions; Time for Reflection and Choice*, 33 PUB. CONT. L.J. 321, 350 (2004) (explaining although "Cold War agencies played a famed role in funding cyber technologies," in fact "the Government's IT workforce, from the start, has been substantially private").

63. *See* P.W. SINGER, CORPORATE WARRIORS: THE RISE OF THE PRIVATIZED MILITARY INDUSTRY 62–64 (2008 ed.) (explaining that "many military functions," especially in IT, "are being transferred to civilian specialists" and "[f]or those who wish to stay at the leading edge of military capabilities, there is a growing need for technical expertise, increasingly from private sources").

64. Moreover, as explained below, *infra* note 194, government contractors are no less susceptible to the preference for the *status quo* software development method or less inclined to suffer from the cultural or bureaucratic resistance to the adoption of agile. So embedded are contractors in the government that they are, in fact, equally part of the problem. Accordingly, this paper makes no distinction between government employees and government contractors.

## II. THE AGILE SOFTWARE DEVELOPMENT METHOD

Before coming to agile, the next three sections will recount what came before, why that did not work, and how this led private industry to innovate. This is more than a history lesson. Understanding the agile method and understanding why the DoD has been a reluctant adopter require an understanding of what agile replaced and why.

### *A. Pre-Agile Software Development Methods*

Since the advent of the computer, there have been three stages of software development. The first was characterized by the lack of any formal methodology and lasted through the 1970s. During this "code and fix" stage, programmers "wrote programs individualistically with little or no planning."[65] This ad hoc method worked well enough at first, but as computing power increased 10,000 fold so also did the complexity of software design, which in turn yielded exponential growth in the "consequences of success or failure."[66] As failing software imposed greater costs, innovators and managers sought to impose order and control costs using new development methods.[67]

The waterfall method was foremost among the new, top-down software-development methods of the second stage. Development was supposed follow an "orderly series of sequential stages," Leffingwell explains, starting with requirements and moving on to design, implementation, testing, and deployment.[68] Notably, its putative founder warned in his first articulation of the waterfall method that it was unsuited to the large projects to which it was later applied *en*

65. *See* Nanda C. Surendra, *Using an Ethnographic Process to Conduct Requirements Analysis for Agile Systems Development*, 9 INFO. TECH. MGMT. 55 (2008).

66. DEAN LEFFINGWELL, AGILE SOFTWARE REQUIREMENTS: LEAN REQUIREMENT PRACTICES FOR TEAMS, PROGRAMS, AND LEFFINGWELL, AGILE SOFTWARE REQUIREMENTS THE ENTERPRISE 3–4 (2011).

67. *Id. But see* Joe Nandhakumar and David E. Avison, *The Fiction of Methodological Development: A Fields Study of Information Systems Development*, 12 INFO. TECH. & PEOPLE 176 (1999) (arguing that methodologies are "a necessary fiction to present an image of control or to provide a symbolic status" and that "formal methodologies are too mechanistic to be of much use in the detailed, day-to-day organization of developers' activities").

68. LEFFINGWELL, AGILE SOFTWARE REQUIREMENTS, *supra* note 66, at 5–6.

*masse*.[69] Waterfall certainly imposed order,[70] but did so at the expense of speed, price, and quality. In many ways, it was worse than what it replaced. Stalin infamously said, "You can't make an omelet without breaking a few eggs."[71] Yet even Stalin would have hated waterfall: eggs were broken, but no omelets were to be had.

Waterfall's failures lay with some faulty assumptions. Most fundamental among these is that requirements can be can be defined and understood before development starts.[72] In fact, requirements are notoriously hard to pin down.[73] The causes for this epistemic problem are complicated,[74] but Don Reinertsen captures well its significance.

---

69. *Id.* (citing Winston W. Royce, *Managing the Development of Large Software Systems: Concepts and Techniques*, 14 WESCON Tech. Papers (1970), *reprinted in* PROCEEDINGS OF THE NINTH INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING (1987)); *see also* CRAIG LARMAN, AGILE AND ITERATIVE DEVELOPMENT: A MANAGER'S GUIDE 105–06 (2004) (suggesting that "few actually read Royce's original waterfall paper" and that "its iterative flavor was lost"); DEAN LEFFINGWELL, SCALING SOFTWARE AGILITY: BEST PRACTICES FOR LARGE ENTERPRISES 17–19 (2007) (explaining that Royce's writings have been "widely misinterpreted").

70. *See* BARRY W. BOEHM, RICHARD TURNER & GRADY BOOCH, BALANCING AGILITY AND DISCIPLINE: A GUIDE FOR THE PERPLEXED (2003) (explaining the benefits of "plan-drive methods" like waterfall are "predictability, stability, and high assurance").

71. *See* Mark Edele, STALINIST SOCIETY: 1928–1953 viii (2011) (explaining that the Stalin quote is actually an "idiomatic translation" of a phrase meaning "if you chop wood, chips will fly").

72. *See* VICTOR SZALVAY, DANUBE TECHS., INC., AN INTRODUCTION TO AGILE SOFTWARE DEVELOPMENT 2 (2004), http://www.danube.com/docs/Intro_to_Agile.pdf (explaining that "one of the biggest problems with waterfall is that it assumes that all project requirements can be accurately gathered at the beginning of the project"); LEFFINGWELL, SCALING SOFTWARE AGILITY, *supra* note 69, at 20–26 (describing the problems with this and three other assumptions in the waterfall model).

73. *See* NORTHERN ET AL., *supra* note 53, at 15 (explaining "the main reason for a high rate of failure in IT development projects" is that such projects are "fraught with uncertainty and ambiguity making it difficult to accurately define the end state up front").

74. The fact that requirements are hard to pin down is partly due to problems with any new technology; customers know it when they see it but seldom know what they want up front. *See* CLAYTON M. CHRISTENSEN, THE INNOVATOR'S DILEMMA: WHEN NEW TECHNOLOGIES CAUSE GREAT FIRMS TO FAIL 147–63 (1997) (arguing market for new technology is unknown and unknowable). And it is also partly due to challenges specific to software development. *See* Szalvay, *supra* note 72, at 3 (arguing "software development is more like new product development than manufacturing" as "building bridges relies on physical and mathematical laws" but programming "has no clear laws or certainties on which to build"); Surendra, *supra* note 65 (noting that developers are enthralled with engineers' "mechanistic view" of development process but instead of designing "buildings and vehicles having relatively predictable requirements, [software] developers need to construct software applications that have *rapidly changing user requirements*") (emphasis added); LEFFINGWELL, SCALING SOFTWARE AGILITY, *supra* note 69, at 21 (explaining the difficulty of defining requirements for intangible creations in comparison with "mechanical and physical devices of the past"); NORTHERN ET AL. *supra* note 53, at 15 (explaining that when designing an "intangible or abstract" product it is "difficult for users to define what they want up front"). *Cf. Fiction and Software*, ECONOMIST, Feb. 8, 2014, at 80–81 (reviewing Vikram

Noting that incorrect requirements accounted for 80%–85% of project failures,[75] he says that the solution was to focus on listening to customers in order to better define their requirements, to which he counters:

> We ignored the fact that many customers don't know what they want. We ignored the fact that even when they know what they want, they can't describe it. We ignored the fact that even when they can describe it, they often describe a proposed solution rather than a real need.

"The sad truth," he concludes, "is that there is no one 'voice of the customer.'" There is instead "a cacophony of voices asking for different things."[76] The effort to perfectly and completely define requirements beforehand is a fool's errand.[77] So waterfall's failure, in large measure, lay with the incorrect assumption that—with enough elbow grease—accurately forecasting requirements was possible.

Compounding this false premise is inflexibility. This likely resulted from waterfall borrowing from manufacturing and construction industries' methods, where "after-the-fact changes are costly, if not impossible."[78] Yet whatever its origin may be, this makes waterfall doubly bad: not only does waterfall start in the wrong direction, it fails to correct course.[79] Nor was it designed to do so. Testing is delayed until it is costly and difficult to make changes.[80] Customers are rarely consulted, usually only once before and once after

---

Chandra's, GEEK SUBLIME: WRITING FICTION, CODING SOFTWARE (2014), which maintains that writing code "stands shoulder to shoulder with art" "[i]n making something out of nothing," unlike the world of architecture and construction, described above, which design buildings and machines that subject to natural laws of the physical world).

75. Don Reinerstein, *Foreword* to LEFFINGWELL, AGILE SOFTWARE REQUIREMENTS, *supra* note 66, at xxiii.

76. *Id.*

77. Some have mocked waterfall as the "requirements, delay, *surprise*" development model. NATIONAL RESEARCH COUNCIL, *supra* note 25, at 47 n.2 (emphasis added). These "unhappy surprises" include "late-breaking negative feedback regarding design commitments that, when learned at a late stage in the process, can be very costly to revise." *Id.* at 47.

78. MARY ANN LAPHAM ET AL., CONSIDERATIONS FOR USING AGILE IN DOD ACQUISITION 6 (2010) (explaining that waterfall borrowed from these industries' production models because there was no other to learn from).

79. *See* Lowell Lindstrom & Ron Jeffries, *Extreme Programming and Agile Software Development Methodologies*, 21 INFO. MGMT. SYS. 41 (2004) (describing rigidity of plan-driven processes).

80. *See* LARMAN, *supra* note 69, at 57–59 (explaining that waterfall puts off testing until the end); LEFFINGWELL, AGILE SOFTWARE REQUIREMENTS, *supra* note 69, at 23–25 (explaining that late changes are technically difficult and costly because "interdependencies have already been built into the system").

development.[81] And the product is released only once.[82] In short, sticking with the plan takes priority, which comes at the expense of the flexibility necessary for a timely response to end user feedback.[83]

A third failing is waterfall's overreliance on documentation. The various steps in the sequential process can be grouped into two main phases: analysis and coding.[84] Months or years are spent on analysis to define and document requirements. Heavy documentation connects the two phases. Yet as Barry Boehm aptly says in his seminal article summarizing the failures of waterfall: "a prototype is worth 100,000 words."[85] He also suggested that too much documentation can also cause "gold plating"[86] and further inflexibility.[87] In sum, waterfall's documentation requirements impose a heavy burden on designers and customers alike that almost certainly outweighs the benefits.

These failings and others[88] made waterfall a flop. Rather than improving on the ad hoc method, development was slower, costlier, and of lower quality.[89] Its shortcomings are well documented.[90] Surprisingly, despite its faults and the introduction of new methods that have proven to work better, waterfall is still widely used in the both private and public sectors.[91]

---

81. *See* Szalvay, *supra* note 71, at 3 (explaining that waterfall asks that customers "specify the entire system without having a chance to periodically see the progress and make adjustments to the requirements as needed").

82. LAPHAM ET AL., *supra* note 78, at 6 (explaining that "one of the primary differences between Waterfall and Agile is the frequency with which usable releases are produced").

83. *See* LEFFINGWELL, SCALING SOFTWARE AGILITY, *supra* note 69, at 21–22 (arguing that the second incorrect assumption underlying waterfall is that "change will be small and manageable").

84. *See* Royce, *supra* note 69.

85. Barry Boehm, *Anchoring the Software Process*, 13 IEEE SOFTWARE 73, 74–75 (1996) (arguing that "written requirements specifications trying to describe the look and feel of a user interface were nowhere near as effective as a user-interface prototype").

86. *Id.* at 74 (arguing that too much documentation "encourage[s] elaborate additions").

87. *Id.* (arguing that fixed requirements "produce point solutions optimized around the original problem statement" that are inflexible and "frequently difficult to modify or to scale up").

88. *See, e.g.*, LEFFINGWELL, SCALING SOFTWARE AGILITY, *supra* note 69, at 22–26 (explaining two more incorrect assumptions of the waterfall method).

89. *See* William H. Roetzheim, *When the Software Becomes a Nightmare: Dealing with Failed Projects*, 13 BUS. L. TODAY 42, 42–43 (2004) (describing the Standish Group's research in the 1990s that "provided concrete evidence of a dirty little secret the information technology community had long suspected—software project failures were rampant and expensive").

90. *See* LARMAN, *supra* note 69, at 74–76 (summarizing four studies on waterfall's failures).

91. *See* LEFFINGWELL, AGILE SOFTWARE REQUIREMENTS, *supra* note 66, at 8–9 (discussing several reasons for waterfall's persistence)

### *B. The Agile Method of Software Development*

Understanding why waterfall failed sets the stage for agile. Whole books are devoted to describing and implementing agile, but its main features can be neatly summarized in three points corresponding to the three main problems with waterfall.

First, agile starts with a premise of epistemic modesty: we cannot know all requirements in advance, despite our best efforts.[92] Explaining how agile corrects for waterfall in this respect, Leffingwell writes, "We do *not* assume that we, or our customers, can fully understand all of the requirements up front, or that anyone can possibly understand them all up front." He continues, "We do *not* assume that change will be small and manageable. Rather, we assume that change will be constant[.]"[93] This may seem like a small difference, but it underpins all that makes agile work so effectively.

Second, agile is above all flexible. It accomplishes this using an iterative process whereby simple versions of the software are delivered early and often.[94] Each iteration includes a compressed version of the various waterfall phases (e.g., design, testing, and feedback),[95] and this cycle is repeated over and over. Mary and Tom Poppendieck describe this iterative process:

> An iteration is a useful increment of software that is designed, programmed, tested, integrated, and delivered during a short, fixed timeframe. It is very similar to a prototype in product development except that an iteration produces a working portion of the final product. This software will be improved in future iterations, but it is a working, tested, integrated code from the beginning.[96]

They explain the significance of this: "Iterations provide a dramatic increase in feedback over sequential software development, thus providing much broader communication" among customers, developers, and other stakeholders."[97] Agile assumes imperfect

92. Richard K. Cheng, *On Being Agile*, NEXTGOV (Sept. 23, 2010), http://www.nextgov.com/defense/2010/09/on-being-agile/47627/ (saying agile is "adaptive" rather than "predictive").

93. LEFFINGWELL, SCALING SOFTWARE AGILITY, *supra* note 69, at 26 (emphasis original).

94. *See* MARY POPPENDIECK & TOM POPPENDIECK, LEAN SOFTWARE DEVELOPMENT: AN AGILE TOOLKIT 27–34 (2003) (explaining that using discrete iterations helps identify "quality problems as soon as they occur"); LARMAN, *supra* note 69, at 9–11; LEFFINGWELL, SCALING SOFTWARE AGILITY, *supra* note 69, at 54 (saying that iterative development eliminates waterfall's attempt to "build it right the first time"); LAPHAM ET AL., *supra* note 78, at 5–6 (explaining the process of focusing efforts by selecting stories from the queue).

95. *See* Szalvay, *supra* note 71, at 4.

96. POPPENDIECK & POPPENDIECK, *supra* note 94, at 28.

97. *Id.*

communication, but constant feedback helps bridge the gap, so that designers eventually come to understand and to provide what the customer actually wants. Agile succeeds so remarkably precisely because multiple failures are expected; designers are expected to fail early and often. Unlike waterfall, "[t]esters are involved from the first iteration" and "[d]esign problems are exposed early," and "change-tolerance is built into the system."[98] This is, Leffingwell writes, "the heartbeat of agility."[99]

Third, agile dumps waterfall's documentation requirements.[100] Instead of such documentation, resources are redirected to developing working prototypes for customers to tinker with—and, again, such "a prototype is worth 100,000 words."[101] Boehm says that "written requirements specifications trying to describe the look and feel of a user interface [are] nowhere near as effective as a user-interface prototype." So the developer's and customer's time is better spent; it is hard—or at least requires a great deal of imagination—to discuss meaningfully how to improve software that does not yet exist. But agile gives customers software they can see, use, and then provide immediate feedback on.

Before proceeding, it seems worth mentioning that agile is more than the latest management-speak patois or business-school gimmick. Some claim that its roots date back to Roman times.[102] It is unclear how tenable that classical pedigree is, and ascertaining agile's genealogy is beyond the scope of this paper. But agile does tap into some basic insights of free-market economics. Its bottom-up approach works for the same reason the free market's "invisible hand" outperforms central planners.[103] Were accurate forecasting possible, waterfall probably

98. *Id.*

99. LEFFINGWELL, AGILE SOFTWARE REQUIREMENTS, *supra* note 66, at 155–69.

100. *See* LARMAN, *supra* note 69, at 326–27 (describing agile documentation methods that reduces preparation time from months or years to hours); LEFFINGWELL, AGILE SOFTWARE REQUIREMENTS, *supra* note 66, at 284 (saying traditional documentation-heavy requirements are "eliminated, reduced in scope, or replaced by lightweight substitutes"); LEFFINGWELL, SCALING SOFTWARE AGILITY, *supra* note 69, at 215–17 (explaining that whereas extensive documentation was "part and parcel of the waterfall model itself," "in agile these documents do not exist").

101. Boehm, *supra* note 85, at 74–75.

102. *See* Reagan & Rico, *supra* note 52, at 50 (claiming agile has roots in Roman legion tactics and experimental techniques used by Leonardo, Newton, Pasteur, and Edison).

103. *See* ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS 35 (R.H. Campbell & R.H. Skinner, eds., 1976) (1776) (first coining the image of the "invisible hand"); *see also* TODD G. BUCHHOLZ, NEW IDEAS FROM DEAD ECONOMISTS 19–25 (1989) (summarizing Smith's "invisible hand" whereby society benefits from each man pursuing his own interests). Incidentally, it is no accident that agile and similar innovations emerged from where they did as "[i]f there is an industry that exemplifies the virtues of the private sector, it is technology." *Companies and the State*, ECONOMIST (SPECIAL REPORT), Feb. 22, 2014, at 12.

would work. Alas, it is not. Therein lies the epistemic problem. Agile takes a more modest approach and avoids that problem, not pretending to know in advance what customers need or want. Instead, it listens, adapts, experiments, and then listens some more. In this way it defers to the wisdom of the masses, and thereby resembles the operation of free markets. Agile is more than a passing fad.

### *C. Agile's Proven Success*

Agile development is not without critics.[104] Nor is there a single method applied uniformly across the field; schisms and heterodoxies abound.[105] This paper does not advocate for any particular sect. Rather, it considers how agile—in a general or ecumenical form— compares with waterfall, and finds that agile has a much better record of success.

Not only does anecdotal evidence suggest that agile works in the private sector, empirical evidence confirms this.[106] For example, a 2004 study by the Standish Group showed that the use of agile cut failure-

104. *See, e.g.*, LAPHAM ET AL., *supra* note 78 at 49–51 (discussing six common objections to agile, especially as applied to the DoD).

105. *See* LEFFINGWELL, AGILE SOFTWARE REQUIREMENTS, *supra* note 66, at 10–29 (describing agile's various forms including iterative/incremental, dynamic systems development method, adaptive software development, extreme programming, open unified process, scrum, lean, crystal methods, and Kanban).

106. *See* LARMAN, *supra* note 69, at 63–109 (providing what Szalvay, *supra* note 72, at 10, calls "the most comprehensive empirical evidence for Agile/Iterative of any book currently on the market," and what LEFFINGWELL, SCALING SOFTWARE AGILITY, *supra* note 69, at 19, calls the best source for "solid, statistical evidence of how [waterfall] fails us again and again") (citing, e.g., Alan D. McCormack, *Product Development Processes that Work*, 42 MIT SLOAN MGMT. REV. 75 (2001) (two-year study by Harvard business professors finding iterative "approach to software development results in speedier process and higher-quality products"); Alan D. MacCormack et al., *Exploring the Trade-offs Between Productivity & Quality in the Selection of Software Development Practices*, 20 IEEE SOFTWARE 78 (2003) (describing results of a follow-up study showing 50% of variation in productivity resulted from two iterative practices—releasing a partial product with lower functionality and daily builds with regression testing); Neil B. Harrison & James O. Complien, *Patterns of Productive Software Organizations*, BELL LABS TECH. J. 140 (1996) (finding a consistent pattern of highly successful software projects where iterative methods were used); David Cohen, Gary Larson & Bill Ware, *Improving Software Investments Through Requirements Validation*, IEEE 26TH SOFTWARE ENGINEERING WORKSHOP 106 (2001) (summarizing study of 400 projects spanning 15 years showing "software pollution" rate was significantly reduced by adopting iterative processes); SHINE TECHNOLOGIES, AGILE METHODOLOGIES SURVEY RESULTS (2003) (describing survey results about agile showing that 88% believed it improved productivity, 84% improved quality); STANDISH GROUP INT'L, CHAOS MANIFESTO 2013, at 5 (2013), http://versionone.com/assets/img/files/ChaosManifesto2013.pdf. (illustrating value of iterative practices following study of 23,000 projects); Andrew Thomas, *IT Projects Sink or Swim*, BRIT. COMPUTER SCI. REV. (2001) (summarizing study of 1,000 UK projects showing 90% of successful projects lasted less than twelve months, and 47% less than six); CAPERS JONES, PATTERNS OF SOFTWARE SYSTEMS FAILURE AND SUCCESS (1996) (large sample study showing that the larger the project, the more likely it will fail)).

rates in half.[107] Their latest report partly attributes increasing success-rates from 29% to 39% from 2004 to 2013 to using agile.[108] Another study claims agile decreased costs by up to 61%, cut delivery time by up to 58%, and reduced defects by up to 81%.[109]

These numbers suggest that if the federal government could successfully implement agile, not only would software quality and delivery times improve, billions in savings would accrue—and not only in the DoD.[110] Critics may object that agile is impossible for the government to implement. In fact, the federal government was a pioneer in iterative software-development methods from 1950s through the 1970s,[111] and there is no reason to think the federal government could not learn to be agile again.[112] Remarkable savings, better value, and faster delivery are within the government's reach.

## III. THE HISTORY OF FEDERAL SOFTWARE PROCUREMENT AND DEVELOPMENT

The previous section detailed the history of the waterfall and agile software-development methods. This section starts with a broad overview the federal government's IT-procurement practices and reforms since the 1960s. Then it describes the government's pioneering efforts with iterative software development (a precursor to agile), its adoption of waterfall and the disastrous consequences that resulted, and finally its long history with agile. This background is necessary to understanding why the federal government, despite the rhetoric about agile methods, is still stuck in the past.

107. Szalvay, *supra* note 72, at 10 (citing STANDISH GROUP INT'L, CHAOS CHRONICLES (2004) (indicating agile reduced failure rates from 31% to 15%)).

108. *See* CHAOS MANIFESTO 2013, *supra* note 106.

109. *See* LAPHAM ET AL. (2010), *supra* note 78, at 36 (citing Jim Highsmith, *Beyond Scope, Schedule, and Cost: Measuring Agile Performance*, Agile Development Conference, Orlando, Florida, 2009)).

110. Perhaps other agencies will require bespoke software less frequently than the DoD; however, to the extent they need software tailored to meet unique needs that are not otherwise supplied in the private market, agile is no less applicable to them and might save additional billions. *See supra* notes 59–60 and accompanying text.

111. *See infra* notes 125–132 and accompanying text.

112. Some have argued that agile only works for smaller organizations or smaller projects. Leffingfwell's entire book, *supra* note 69, is devoted to arguing that agile can work on a larger scale and for large enterprises. The federal government and the DoD should be no exception.

### *A. An Overview of IT Procurement Policy Since the 1960s*

From the 1965 until 1996, the General Services Administration exercised central control over IT purchases.[113] With the Clinger–Cohen Act's repeal of the Brooks Act,[114] IT purchasing reverted to individual agencies,[115] and IT- and non-IT processes were thereby merged because it was thought that having separate processes was too "cumbersome and slow."[116] Since then, IT purchases, both hardware and software,[117] are done using "normal procurement procedures following a few special rules in FAR 39."[118]

While agencies have purchasing authority, the Office of Management and Budget still has responsibility over standards and policy.[119] Congress has also established a number of requirements: that agencies have a Chief Information Officer,[120] follow planning requirements,[121] and use modular contracts.[122] It has also required OMB to promote various contract-management programs.[123]

### *B. The Federal Government's Experience with Iterative, Waterfall, and Agile Software Development Methods*

Some may suppose the government cannot do agile either because of its size or to inherent limitations on the public sector's efficiency or

---

113. 40 U.S.C. § 759 (1995); *see also* John, *supra* note 47, at 4, 7–8 (describing the United States' failed experiment with consolidated IT from the mid-1960s until 1994).

114. Information Technology Management Reform Act of 1996, Pub. L. No. 104-106, div. E, tit. LI, § 5101, 110 Stat. 186, 680 (1996) (codified at 40 U.S.C. § 11302).

115. 40 U.S.C. § 11314 (2013).

116. NATIONAL RESEARCH COUNCIL, *supra* note 42, at 28.

117. 48 C.F.R. § 2.101 (2014).

118. JOHN CIBINIC, JR., RALPH C. NASH & CHRISTOPHER R. YUKINS, FORMATION OF GOVERNMENT CONTRACTS 1104 (4th ed. 2011). (referencing 48 C.F.R. pt. 39).

119. *Id.* at 1104–05 (citing 44 U.S.C. § 3504(h); 40 U.S.C. § 11302(b); OMB Circular A-130, http://www.whitehouse.gov/omb/circulars_a130_a130trans4).

120. 40 U.S.C. § 11315 (2013).

121. *Id.* § 11312(b); *see also* OMB Circular A-130, *supra* note 119, at ¶ 8.b(4); 48 C.F.R. § 39.102 (2014) (establishing that agencies should consider "risks, benefits, and costs" of IT).

122. 41 U.S.C. § 2308 (2013) (mandating modular systems); see also CIBINIC ET AL., *supra* note 118, at 1108–09 (explaining that modular contracts are "successive acquisitions of interoperable increments"). *But see Acquisition White Paper on Modular Contracting* (Jul. 26, 1997) (GSA's warning about risks of modular contracting because modules may not be fully compatible).

123. *See* 40 U.S.C. § 11303 (requiring OMB to encourage performance- and results-based management for agency IT purchases); § 11302(b) (promotion of acquisition and capital planning processes); § 11312 (detailing capital planning and investment control); § 11313 (describing performance- and results-based management); *see also* OMB Circular A-130, *supra* note 119, at ¶ 8.b(1) (implementing these policies).

competency.[124] In fact, not only is the government capable of using agile, it was a pioneer in the use of iterative and incremental methods that were the precursors to agile. For example, for several decades starting in the 1950s, the DoD used these methods to develop software for weapons systems including the Army's artillery command-and-control system,[125] the Navy's Trident submarine,[126] and LAMPS helicopter-ship system,[127] and the Air Force's air defense system.[128] The DoD was not alone. NASA used such methods for the Project Mercury, the first manned spaceflight program,[129] and for the space shuttle.[130]

These were not exceptions. Larman explains that IBM's Federal Services Division and its rival developer, TRW, frequently used incremental methods in the 1970s and that their use was "a well-known practice."[131] Finally, the use of iterative engineering methods was not limited only to software development. For example, the Air Force utilized lean or agile manufacturing methods "to usher in the jet age and to rapidly evolve experimental aircraft such as X-15, SR-71, U-2, F-111, F-117, and many others."[132] Such methods are considered close cousins, if not parents, to agile software-development methods.[133]

---

124. *See supra* note 112.

125. Doris Tamanaha, *An Integrated Rapid Prototyping Methodology for Command and Control Systems*, 7 ACM SIGSOFT SOFTWARE ENGINEERING NOTES 169 (1982) (describing Army project using iterative methods for designing software for artillery command and control in 1984–88)).

126. Don O'Neil, J. OF SYSTEMS & SOFTWARE 77 (1983) (relating the use of iterative software methods for development of the Trident submarine in 1972).

127. *See* LARMAN, *supra* note 69, at 83–84 (describing a four-year, 200 person project with millions of lines of code that whose every delivery "was on time and under budget").

128. *See* Carolyn Wong, A Successful Software Development, 10 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 714–27 (1984) (describing the use of iterative methods to develop the air defense system in 1977–80 and their initial problems with developing complex software using waterfall).

129. *See* LARMAN, *supra* note 69, at 79–81 (citing Craig Larman & Victor Basili, *Iterative and Incremental Development: A Brief History*, 36 COMPUTER 47 (2003) (describing incremental software methods used in Project Mercury in the 1950s)).

130. William A Madden & Kyle Y. Rone, *Design, Development, Integration: Space Shuttle Primary Flight Software System*, 27 COMMUNICATIONS OF THE ACM 14 (1984) (describing NASA's use of iterative approach for space shuttle's flight software system in 1977–80 as waterfall method was unsuitable given the frequently changing requirements of such a complex system).

131. LARMAN, *supra* note 69, at 82–84 (describing TRW's work on the Army's ballistic missile defense system in the 1970s) (citing R.D. Williams, *Managing the Development of Reliable Software*, *in* PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON RELIABLE SOFTWARE (1975)).

132. *Id.* at 51.

133. *Id.*

For reasons that remain unclear, the DoD mandated use of waterfall methods in the 1980s.[134] Efficiency suffered.[135] The implementation under DoD-STD-2167 provide a striking case study of waterfall's shortcomings: "Out of a total cost of $37 billion for the sample set, 75% of the projects failed or were never used, and only 2% were used without extensive modification."[136] "DoD planners came to believe that the key to successful weapon systems was to apply rigid manufacturing principles to acquisition and systems engineering."[137] Thus, a series of tightly controlled procurement regulations was instituted, which lasted until the mid-1990s.[138] This was typical of a government that had lost its way and had forgotten about the virtue of iterative development methods[139]—to the detriment of end-users and the public fisc.[140]

For much of the 1980s, waterfall was mandatory for the DoD's software development and procurement.[141] Later in the decade, following the "stultifying influence" of waterfall on large IT projects, those requirements were lifted and a new standard adopted to allow for use of iterative and incremental methods.[142] Despite this, the regulation

134. For a possible explanation, see *infra* note 137.

135. LARMAN, *supra* note 69, at 76 (citing R. Solon, *Benchmarking the ROI from Software Process Improvement*, 5 DOD SOFTWARE TECH. NEWS 6 (2002) (study of 43,700 projects showed not only that agile was more efficient than lean but that only "loosely" applying waterfall method caused significant productivity improvements)).

136. *Id.* at 87 (citing Lt Col (ret.) Joe Jarzombek, *The 5th Annual JAWS S3 Proceedings* (1999)).

137. Reagan & Rico, *supra* note 52, at 51. It would be an interesting historical or sociological question to consider whether the adoption of top-down controls was considered necessary following the Sputnik scare in 1957. We now know that Soviet Union would later collapse in part because it could not keep up with the rapid growth in Western technology. So it seems strange in hindsight that we might have adopted authoritarian methods to expedite defense acquisition and technological development. Yet that strangeness is anachronistic. At the time it might have seemed that top-down controls were necessary in order to keep up with our Cold War rival, which was unfettered by free-market economics and, thus, winning the space race. *See, e.g.*, PAUL DICKSON, SPUTNIK: THE SHOCK OF THE CENTURY 223–24 (2011) (describing the clamor for radical changes to U.S. policy in order to keep up with Russian technology).

138. LARMAN, *supra* note 69, at 87 (citing four DoD regulations and explaining that "these were only the tip of an iceberg of thousands of lower-level standards making up . . . the defense acquisition system").

139. *See id.* at 85–87 (citing U.S. GOV'T ACCOUNTING OFFICE, AIR TRAFFIC CONTROL EVOLUTION AND STATUS OF FAA'S AUTOMATION PROGRAM, GAO/T-RCED/AIMD-98-85 (1998) (describing the FAA's disastrous efforts to design a new air traffic control system using the waterfall method resulting in $2.6 billion spent and nothing to show for it)).

140. Larman explains that prior to waterfall, iterative and ad hoc methods coexisted. *See id.* at 102 (explaining that iterative was a "contemporary alternative" with ad hoc).

141. *Id.* at 87 (citing DOD-STD-2167).

142. *Id.* at 88–89 (adopting DOD-STD-2167 in February 1988).

"contain[ed] an implied preference for the waterfall model, due to its document-driven milestones approach."[143]

After years of failure with waterfall, a 1994 study recommended iterative methods.[144] Soon after, a regulation was introduced removing any bias favoring waterfall.[145] Six years later, a new instruction was introduced, which again recommended iterative methods.[146]

In 2003, the DoD implemented a "multiple milestone" process that introduced more flexibility into acquisition processes.[147] Dissatisfaction with this process led to further revisions in 2007 and 2008[148] to what are commonly called the DoD 5000 series. Though these regulations both mentioned and recommended agile-like methods,[149] they were still blamed for insufficiently clearing the path for agile reforms.[150]

In March 2009, the Defense Science Board found the conventional procurement system was "inadequate" for cyber acquisitions because of the "short half-life" of commercial IT.[151] This report encouraged further agile reforms in Congress.[152] On October 9, 2009, President Obama signed the National Defense Authorization Act (NDAA) of 2010,[153] which mandated agile procurement methods.[154] Thirteen months later, the DoD's report to Congress again promised its recent reforms would "enable DoD information capability projects to take advantage of the benefits of agile development methods[.]"[155] Congress

143. *Id.* at 89.

144. LARMAN, *supra* note 69, at 89–90 (citing REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON ACQUIRING DEFENSE SOFTWARE COMMERCIALLY (1994)).

145. *Id.* at 90 (citing MIL-STD-498 (Dec. 1994) (establishing uniform requirements for software documentation and development)).

146. *Id.* (referencing DoDI 5000.2).

147. DEFENSE SCIENCE BOARD REPORT, *supra* note 25, at 29–30.

148. *Id.* at 30–32.

149. *See* DoDD 5000.01, § 4.3.2 (replacing "spiral" from the previous version with "incremental" as the "preferred" development method for advanced technology); DODI 5000.02, Enclosure 2, ¶ 5.a (describing the technology development phase as "iterative").

150. *See, e.g.*, LAPHAM ET AL., *supra* note 78, at 12–13 (noting a "strong belief that is prevalent across the DoD community" is that the DoD 5000 series is "rigid in requiring a traditional Waterfall process for the development of software").

151. *Id.* at ix.

152. *See id.* at 42–45 (citing several studies since the Goldwater-Nichols legislation in 1986 stressing the need for acquisitions reform).

153. *See* Cheng, *supra* note 92.

154. National Defense Authorization Act (NDAA) for Fiscal Year 2010, Pub. L. No. 111-84, 123 Stat. 2190 (2009).

155. OFFICE OF THE SECRETARY OF DEFENSE, A NEW APPROACH FOR DELIVERING INFORMATION TECHNOLOGY CAPABILITIES IN THE DEPARTMENT OF DEFENSE 12 (2012) (report to Congress pursuant to Section 804 of the National Defense Authorization Act of 2010).

considered yet another IT reform bill in 2013: the Federal Information Technology Acquisition Reform Act (FITARA). It was originally an independent bill, was added to the National Defense Authorization Act (NDAA) of 2014, and was finally removed for additional consideration.[156]

The DoD has taken clandestine efforts toward rapid cyber procurement, but secrecy makes it hard to appraise their efficacy.[157] If the past is any guide, the results may be underwhelming. For some time the DoD has spoken the language of agile[158] without actually doing or being agile. Though words like "agile" and "lean" may dominate DoD press releases about improving cyber-procurement methods, there is little show for this rhetorical flourish, at least not at the DoD-wide level.

Although the DoD as a whole has yet to fully implement its agile ideals, some individual services have taken steps in that direction. For example, on November 28, 2005, the Secretary of the Air Force signed a memo directing the use of lean methods,[159] and his successor signed an acquisition improvement plan on May 4, 2009, which also featured

156. FITARA was originally H.R. 1232, but on June 14, 2013 the House approved adding it as an amendment to the NDAA of 2014. David Perera, *House Approves FITARA Version as Part of National Defense Bill*, FIERCEGOVERNMENTIT (June 17, 2013), http://www.fiercegovernmentit.com/story/house-approves-fitara-version-part-national-defense-bill/2013-06-17; Dietrich Knauth, *Congress Prepares Last-Ditch Attempt At Defense Policy Bill*, LAW360 (Dec. 9, 2013), http://www.law360.com/articles/494217/congress-prepares-last-ditch-attempt-at-defense-policy-bill (explaining other aspects of the NDAA held up its passage and it appears that lawmakers will reach an agreement before the bill expires). Ultimately, Congress removed FITARA from the 2014 NDAA, and postponed its consideration. Dietrich Knauth, *Government Contracts Regulation And Legislation To Watch in 2014*, LAW360 (Jan. 1, 2014) (explaining that the delay was caused in part by worries about the rollout of Heathcare.gov and a consensus that "the way the government buys technology is too slow, too burdened by inefficiencies and too prone to high-profile failures").

157. *See, e.g.*, Ellen Nakashima, *Pentagon to Fast-Track Cyberweapons Acquisition*, WASH. POST (Apr. 9, 2012), http://articles.washingtonpost.com/2012-04-09/world/35453841_1_weapon-systems-pentagon-technology-and-logistics (reporting on this development from an undisclosed 16-page Pentagon report describing a new rapid cyber procurement program).

158. "Agile" has become a popular word in defense circles, and has lost currency with repetition. *See, e.g.*, QUADRENNIAL, *supra* note 28, at 1, 73, 81, 103 (using "agile" four times); DEPARTMENT OF DEFENSE STRATEGIC MANAGEMENT PLAN FY 2012–FY 2013, at 2, 6, 12, 24, 37 (using "agile" seven times and describing two of its seven goals using that adjective); DEFENSE INFORMATION SYSTEMS AGENCY STRATEGIC PLAN: 2013–2018, at 2, 4–5, 10, 14 (2013) (using "agile" six times).

159. *See* LEFFINGWELL, AGILE SOFTWARE REQUIREMENTS, *supra* note 66 (equating lean and agile); *Information Technology Lean Process Streamlines Acquisition*, U.S. FED. NEWS (Jan. 23, 2006), *available at* 2006 WLNR 2114017 (reporting that Secretary Michael Wynne signed a memo directing use of lean acquisition methods).

agile methods.[160] Such initiatives have proven more than empty slogans and have led to pockets of success.[161] Lapham cites the Air Force's FIST program and recommend duplicating its success with smaller teams.[162] The Air Force's Electronic Systems Center (ESC) at Hanscom AFB, Massachusetts announced it had started to develop capabilities in order to "to fill technology gaps within hours or weeks."[163] And the Army is fielding a new agile system for its communications-networks acquisitions.[164]

Unfortunately, although the authority to use iterative methods has been available for nearly two decades,[165] the programs listed in the last paragraph are exceptions. To date, agile reforms have been meager.[166] This should come as no surprise because companies and cultures "emphasiz[ing] hierarchical management and control, and detailed predictive planning [are] the slowest adopters" of agile, and few institutions are more hierarchical than the DoD.[167] The next section considers such cultural impediments and other reasons agile has not taken root and makes suggestions for improvement.

160. AIR FORCE ACQUISITION IMPROVEMENT PLAN 6 (2009) (favoring an "incremental acquisition strategy" whereby "early, if only partial, operational capabilit[ies] [are] pursued rather than strategies that deliver the 100% solution[s]" that are too costly, late, or risky).

161. *See, e.g.*, LAPHAM, *supra* note 53, at 2 (describing interviews with successful agile programs used in preparing report: "Joint Mission Planning System (JMPS), Single Integrated Air Picture (SIAP), Operationally Responsive Space (ORS), Virtual Mission Operations Center (VMOC), Space Radar, an Army tank program, and some other classified programs").

162. *Id.* at 43.

163. *See* Brewin, *supra* note 52. ESC has since been reorganized under the Air Force Material Command's new Life Cycle Management Center (LCMC). *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-366, AIR FORCE ELECTRONIC SYSTEMS CENTER (2013) (detailing the reorganization of Hanscom AFB's under LCMC).

164. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-179, ARMY NETWORK: SIZE AND SCOPE OF MODERNIZATION INVESTMENT MERIT INCREASED OVERSIGHT (2013).

165. *See supra* notes 145–146 and accompanying text.

166. *See, e.g.*, Porche et al., *supra* note 53, at xiv (acknowledging that agile reforms will not be easy for the Navy); Reagan & Rico, *supra* note 52, at 52 (arguing iterative methods are here to stay, but "there is a long way to go" in terms of implementing such reforms); *Air Force Materiel Command Building Acquisition Plan For Cyber Purchases*, 20 INSIDE THE AIR FORCE (Dec. 18, 2009), *available at* 2009 WLNR 25490253 (AFMC commander acknowledging that the Air Force had not figured out how to do agile cyber procurement); Teri Takai, *DoD CIO's 10-Point Plan for IT Modernization* (2012) (urging agile acquisitions reforms), http://dodcio.defense.gov/Portals/0/Documents/ITMod/CIO%2010%20Point%20Plan%20for%20IT%20Modernization.pdf.

167. LARMAN, *supra* note 69, at 87.

## IV. PROBLEMS WITH ADOPTING AGILE IN THE DOD AND HOW TO FIX THEM

This closing section first demonstrates that DoD software development still uses the waterfall. Despite numerous initiatives and much rhetoric, agile has not been widely adopted. It then presents studies showing that laws or regulations are not the primary reason. This is mainly a function of culture. It offers suggestions for changing the culture. It closes with some laws and regulations that could be amended to more fully promote agile reform.

### *A. DoD Software Development Still Resembles The Waterfall Method*

Notwithstanding recent changes in the laws and regulations governing acquisitions supposedly implementing agile, the DoD is still doing waterfall. For simplicity, this section will focus on the same three shortcomings listed above to illustrate how much the DoD still uses waterfall: a faulty assumption about what can be known beforehand about requirements; inflexibility after coding has begun; and onerous documentation requirements.

First, though the DoD purports to be agile, it relies on lengthy up-front analysis to define requirements. "Current DoD processes," the National Research Council explains, "put great emphasis on detailing requirements before a program is approved to start," that results in "years of requirements development" and in turn leads to "the delivery of IT systems that are trying to meet requirements that have long since changed or are continuing to shift."[168]

Two examples illustrate the tendency to ignore or misunderstand the application of agile to DoD IT acquisition. One is the Air Force's Acquisition Improvement Plan. Though praised above for promoting agile,[169] this plan also displays a certain cognitive dissonance. It uses some agile jargon,[170] yet on closer inspection its wording and guidance

168. NATIONAL RESEARCH COUNCIL, *supra* note 42, at 41; *id.* at 85 (recommending that "big-R" replace "small-R" requirements, meaning that "high-level descriptions that are expected to be fairly stable" replace "more detailed requirements" that "evolve" as development progresses).

169. *See* AIR FORCE ACQUISITION IMPROVEMENT PLAN, *supra* note 160.

170. *Compare id.* ("warfighters must resist the temptation to pursue high risk requirements that are too costly and take too long to deliver in favor of an incremental acquisition strategy" and favoring "incremental strategies that deliver early, if only partial, capabilities") *with* 1 (implying that requirement can be forecasted by faulting the current system for "requirements continu[ing] to creep well beyond their initial scope), 2 (citing a study faulting the Air Force for having "unstable requirements" implying that requirements can be predicted and controlled), 5–6 (discussing requirements generation and in addition to the agile-friendly language quoted above

sound more like waterfall. To be fair, this is complicated by the fact that this document refers to defense acquisition generally and not only to IT acquisition.[171] Yet there is still a glaring inconsistency.

The other is the DoD's report to Congress in response to Section 804 of the NDAA of 2010[172] mandating agile IT acquisition. Though it uses words like "agile" or "iterative" repeatedly,[173] devotes 61 pages to planning for agile,[174] and starts strong on requirements development,[175] it quickly becomes clear that the requirements process is *not* agile, iterative, or simple. One is soon lost in a sea of acronyms and abbreviations for the various steps.[176] Earlier the report failed to conceal its pining for the waterfall metrics of yore, listing among its accomplishments "well-scoped and well-defined requirements."[177] Either the authors did not recognize the inconsistency[178] or they are

making several recommendations more in keeping with waterfall, e.g., saying requirements generation must occur "early" and be a cross-functional endeavor, implying this is a lengthy process balancing several competing objectives), 7 (mandating that requirements be "finite, measurable, [and] prioritized," again taking as given that creating such a list of requirements is desirable), and 7 ("freez[ing] program requirements at contract award," once again making the assumption that requirements can be forecasted).

171. *See, e.g.*, NATIONAL RESEARCH COUNCIL, *supra* note 42, at 40–41 (conceding that the DoD's caution and "emphasis on detailing requirements before a program is approved to start" might make sense for major weapons systems, but arguing that is unsuitable to IT acquisitions).

172. NDAA for Fiscal Year 2010, Pub. L. No. 111–84, § 804, 123 Stat. 2190, 2402–03 (2009) ("Implementation of New Acquisition Process for Information Technology Systems").

173. *See* A NEW APPROACH FOR DELIVERING INFORMATION TECHNOLOGY CAPABILITIES IN THE DOD, *supra* note 155, at 7, 9, 12 (using "agile" three times); *id.* at 2, 4, 8–10, 17 (using "iterative" six times).

174. *See, e.g.*, *id.* at 12 (assuring Congress that new common infrastructure will enable the DoD "to take advantage of the benefits of agile development methods").

175. *Id*. at 14–15 (noting new process "will need to acknowledge the uncertainty associated with the dynamic IT environment and incorporate the flexibility").

176. "Initial requirements will be defined at the mission level[.]" *Id.* at 15. In addition to a half dozen other requirements, these broad requirement definitions will include "key performance parameters approved by the Joint Requirements Oversight Council (JROC)[.]" *Id.* Processes will differ by area, but "all processes will include business process reengineering and an implementation management plan describing all DOTMLPF actions necessary to prepare the user community before receiving the IT capability." *Id.* Requirements must also be run through the "JCIDS process to streamline requirements." *Id.* DoD business software must also be run through the Business Capability Lifecycle (BCL). *Id.* at 16. Several changes are specifically mandated in Section 804. For example, instead of "traditional acquisition project milestones," under the new reforms these will be replaced by "in-process reviews by integrated governance councils with decision authority[.]" *Id.* In short, this is still a very complicated requirements development process more akin to the waterfall than to the agile method it espouses.

177. *Id.* at 4.

178. That is, if requirements can be accurately "scoped" or "defined" then why use agile? The inability to perfectly requirements is what makes agile necessary in the first place.

passive–aggressive, using the agile terminology but atavistically clinging to waterfall practices.[179]

Second, studies suggest the DoD is still locked into a rigid process that is inflexible once coding has started.[180] Anecdotal evidence also suggests this is the case, given top officials quoted above on continuing problems with slow cyber procurement.[181]

Third, the DoD still requires reams of documentation. Contractors who are familiar with agile and then work with the DoD complain that the DoD wants to have its cake and eat it, too.[182] It calls itself agile but uses the paperwork that was the hallmark of waterfall; it's business as usual. Documentation "generated for agile is tailored to meet the minimum required" by developers, whereas "the DoD still rel[ies] heavily upon milestone reviews,[183] documents, reports, and selected metrics."[184] Over-documentation reflects the false premise about requirements; much effort goes into "granular" estimates and forecasts for the Integrated Master Schedule.[185] Program managers also demand the "full complement" of documentation to show progress.[186] Thus, a common complaint among contractors is that the government has not

179. Lapham suggests a third option. Organizations undergoing transformational change that comes with adopting a new business model often go through a period where their "espoused values" fail to align with "basic assumptions." LAPHAM, *supra* note 53, at 18–19 (citing EDGAR H. SCHEIN, ORGANIZATIONAL CULTURE AND LEADERSHIP (1992)). Perhaps this is not only a more charitable explanation but also more accurate.

180. Mary Lapham, *DoD Agile Adoption: Necessary Considerations, Concerns, and Changes*, CROSSTALK 31 (Jan. 2012), http://www.crosstalkonline.org/storage/issue-archives/2012/201201/201201-Lapham.pdf (summarizing a Carnegie-Mellon Software Engineering Institute (SEI) study and describing some cultural barriers to full implementation of agile in the DoD); U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-681, EFFECTIVE PRACTICES AND FEDERAL CHALLENGES IN APPLYING AGILE METHODS (2012) (explaining various obstacles in shifting from waterfall to more flexible agile methods); LAPHAM, *supra* 53, at 14 (explaining that adopting agile processes to replace waterfall will require substantial cultural change within the DoD).

181. *See generally supra* note 52 (quoting a half dozen commentators and officials on how slow DoD IT acquisition process is); *see also* Clark, *supra* note 46 (top cyber commander saying "he wanted to buy 'faster, better, quicker' since the cyber realm doesn't really allow for the seven to 10 years a standard acquisition program usually takes."); INSIDE THE AIR FORCE, *supra* note 166 (Air Force general officer acknowledging that Air Force still has not figured out how to do rapid cyber procurement).

182. *But see infra* note 194.

183. Agile proponents mock such documentation, which agile methods render superfluous, as "high ritual" or "high ceremony." *See* LAPHAM, *supra* note 53, at 37 (citing ALISTAIR COCKBURN, AGILE SOFTWARE DEVELOPMENT: THE COOPERATIVE GAME (2006 2d ed.)).

184. William Broadus, *The Challenges of Being Agile*, DEF. AT&L 5, 8 (Jan. 2013).

185. LAPHAM ET AL., *supra* note 78, at 17.

186. *Id.* at 18.

adjusted its documentation requirements to correspond to supposedly agile methods.[187]

As described above, agile addresses each of these three shortcomings. Were it applied in substance as well as in name, the DoD would profit from lower prices, timelier delivery, and better products. So what is keeping the DoD from doing agile? The next section tries to answer that question.

### *B. Federal Law or Regulations Do Not Preclude Agile; Instead, Culture and Bureaucratic Inertia Impede Change*

After several decades of IT-acquisition reforms one thing is clear. The problem is not laws or regulations that favor waterfall or disfavor agile. Agile has been an option under the rules for nearly two decades.[188] Several studies have found that the current set of procurement laws and regulations are not incompatible with agile.[189] Though perhaps not tailored as well as they could be, which the next section considers, that is not the main problem.

The main problem, instead, lies with the culture.[190] As Lapham writes, "Agile culture runs counter to the traditional DoD acquisition culture in many ways."[191] This section considers four reasons why the DoD culture favors waterfall: a preference for familiar hierarchical control, risk aversion, and ignorance of the legal authority permitting

187. *Id.* at 40–41. *But see infra* note 194.

188. *See supra* notes 145–146 and accompanying text.

189. LAPHAM, *supra* note 53, at 42 (saying that while many in the acquisition community fear that agile is forbidden, "we do not know of any regulations that expressly preclude or limit the use of Agile"); LAPHAM ET AL., *supra* note 78, at 12–13 (noting that although there is a widespread belief that the DoD 5000 series forbid agile "programs that have used Agile in software development have found that the DoD 5000 series has great flexibility and does not in fact preclude the use of Agile"); Broadus, *supra* note 184, at 6 (citing "multiple studies" indicating that "there are no direct policy or practice issues that would preclude or limit the use of Agile methods within the DoD"); NORTHERN ET AL., *supra* note 53, at 24 (citing Duquette, Bloom, & Crawford, *Transitioning Agile/Rapid Acquisition initiatives to the Warfighter*, The MITRE Corporation, Technical Report WN080041 (2008) (unpublished) (citing specific provisions from the FAR and explaining how they support agile contracting, specifically §§ 6.3, 16.207, 16.5, 16.603, 43.2).

190. *See* NATIONAL RESEARCH COUNCIL, *supra* note 42, at 40–42 (describing "cultural impediments take precedence over rapid [software] development"); STAFF OF. S. SUBCOMM. ON INVESTIGATIONS, COMM. ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS, 113TH CONG., REP. ON THE AIR FORCE'S EXPEDITIONARY COMBAT SUPPORT SYSTEM: A CAUTIONARY TALE ON THE NEED FOR BUSINESS PROCESS REENGINEERING AND COMPLYING WITH ACQUISITION BEST PRACTICES 1–2, 8, 18–20 (Jul. 7, 2014) (attributing the failed development of logistics software to "resist[ing] institutional changes necessary for success" and "cultural resistance to change").

191. LAPHAM, *supra* note 53, at 21.

agile methods.[192] Before proceeding, it bears mentioning that cultural issues are not unique to the military; recognizing the corporate culture is increasingly recognized by business scholars as an important part of what executives do, and can help them to benefit from and, where necessary, change or compensate for that culture.[193]

First, maybe senior procurement personnel have resisted agile since they grew up with and are comfortable with waterfall.[194] After all, waterfall was not only preferred in the 1980s, it was required.[195] Thus, Lapham describes a culture both "heavily invested" in waterfall and "skeptical" about agile,[196] and attributes this to comfort with the status quo.[197] It bears mentioning that the DoD is not unique in this respect; agile acolytes have long evangelized that it is not enough to do agile, but that organizations must develop an agile culture.[198]

The tendency to treat software development like any other large weapons-systems procurement is a kindred problem. As the National Research Council explains, "DOD systems acquisition policies,

192. These are not the only reasons that the DoD acquisition community prefers the status quo and disfavors agile. There are several other reasons. *See, e.g.*, LAPHAM ET AL., *supra* note 78, at 49–51 (listing six common complaints about agile methods among DoD contracting professionals including that it is new, risky, and difficult to adopt); LAPHAM, *supra* note 53, at 18–22 (identifying the DoD's general cultural resistance to agile methods). And in addition to cultural resistance to agile, the workforce has several other shortcomings. *See, e.g.*, NATIONAL RESEARCH COUNCIL, *supra* note 42, at 42–43 (listing several such problems, including "personnel practices that are common in the acquisition community" such as "rotating personnel too often" for program managers to see a project through to completion).

193. *See Learning the Lingo*, ECONOMIST, Jan. 11, 2014, at 72–73 (reviewing a new book on the subject, JOHN CHILDRESS, LEVERAGE: THE CEO'S GUIDE CORPORATE CULTURE (2013)); *Crossing the Divide*, ECONOMIST, Oct. 12, 2013, at 99–100 (reviewing a book on how national cultures affect corporate cultures, KAI HAMMERICH & RICHARD LEWIS, FISH CAN'T SEE WATER, HOW NATIONAL CULTURES CAN MAKE OR BREAK YOUR CORPORATE STRATEGY (2013)).

194. LAPHAM, *supra* note 53, at 14. Lapham also explains that DoD acquisition personnel are not alone in this regard. She writes, "long-time DoD contractors" are likewise "more comfortable with Waterfall and skeptical about using Agile." LAPHAM ET AL., *supra* note 78, at 12.

195. *See supra* note 134.

196. LAPHAM ET AL., *supra* note 78, at 43.

197. *Id.* (writing that "culture of the DoD acquisition community . . . is *comfortable* with Waterfall and skeptical about the use of Agile") (emphasis added).

198. *See, e.g.*, LAPHAM, *supra* note 53, at 1–2, 13–15 (describing the so-called "Agile Manifesto" and the challenges of not just "doing" agile but also "being" agile, i.e., developing an agile culture); LAPHAM ET AL., *supra* note 78, at 43 (relating that a frequent topics at the 2009 Agile Development Practices Conference was culture and that the that agile "d[oes] not succeed if an organization's culture d[oes] not support it"); LARMAN, *supra* note 69, at 34 (describing the importance of a firm's culture to the agile method); LEFFINGWELL, SCALING SOFTWARE AGILITY, *supra* note 69, at 92 (describing corporate culture as a fundamental impediment to agile methods); LEFFINGWELL, AGILE SOFTWARE REQUIREMENTS, *supra* note 66, at 391 (describing agile culture as a fundamental principle of the agile method).

expertise, practice, and *culture*—including those applied to IT systems—reflect the practices, policies, and *cultural* norms associated with large weapons systems programs."[199] The problem is those methods are incongruous with challenges unique to software; software development is not major weapons acquisitions. Continuing, the National Research Council explains, "there is a long-standing reluctance to deviate from standard weapons system acquisition processes, and acquisition personnel are not trained or led to differentiate the unique aspects of IT systems acquisition."[200] So DoD procurement personnel resist treating software differently from what they know best: the sequential methods used for other acquisitions.[201]

Second, to restate an obvious point mentioned above, the DoD is by its very nature a hierarchical organization.[202] So too is its acquisition culture.[203] Thus, agile methods clash with that culture, the former being bottom-up and latter top-down. And it would thus seem that DoD personnel may prefer the sense of control that waterfall confers: plans are made from on high, the design follows strict requirements, and delivery is to conform with the plan.[204]

Third, caution also plays a role. Project managers are used to "following [a] plan with minimal change," whereas agile "focuses on adapting successfully to inevitable changes."[205] It isn't only that waterfall is more familiar, but also that waterfall is considered safer—a stable option with fewer risks is alluring. As the incumbent, it may seem "safe" or "conservative," but this is illusory. In fact, choosing waterfall is a "dangerous decision that can drastically increase programmatic risk" and too often results in "total project failure."[206] Yet this is often lost on the putatively risk averse.

---

199. NATIONAL RESEARCH COUNCIL, *supra* note 42, at 4 (emphasis added).

200. *Id.* at 33.

201. LAPHAM, *supra* note 53, at 14 (recounting DoD's "longstanding reluctance to deviate from standard weapons system acquisition processes," which generally use waterfall).

202. *See supra* note 167 and accompanying text.

203. *See* NATIONAL RESEARCH COUNCIL, *supra* note 42, at 40–41 (explaining that the DoD prefers waterfall's hierarchical structure); DEFENSE SCIENCE BOARD REPORT, *supra* note 25, at 37–38 (describing "log jams" and bureaucratic processes whereby myriad functional organizations can slow down or even stop programs that do not satisfy their concerns).

204. That is not to say there are not reasons for its hierarchical culture. "Given the criticality and danger of its mission, its worldwide operations and large workforce, and the frequent need for clear, decisive action, the Department of Defense, by its nature, is an organization with a classic command-and-control culture." NATIONAL RESEARCH COUNCIL, *supra* note 42, at 40.

205. *Id.* at 40–41; *see also* Broadus, *supra* note 184, at 9 (contrasting traditional DoD culture where "the focus is on following the plan with minimal change" with agile procurement where "the focus is on adapting successfully to inevitable change").

206. NATIONAL RESEARCH COUNCIL, *supra* note 25, at 47.

Finally, ignorance of what the procurement laws and regulations allow, though not purely a cultural issue, has discouraged the use of agile. Although statutes and regulations have allowed iterative methods for nearly two decades, this confusion still exists.[207] Lapham cites a "widespread perception" that agile conflicts with DFARS 5000.01 and 5000.02,[208] when that is not the case.[209] DoD contractors share this confusion.[210] Thus, ignorance remains a problem.

Because the problem is mainly cultural, tweaking the regulations is not the solution; the people matter far more than the policy. Agile reforms will not work until the culture changes. Procurement professionals must know their options, must understand what agile is, and must be committed to applying it. This is mainly a function of better training, which may include better centralized training[211] or "embedded" agile experts to assist with training.[212] Lapham suggests that in order to change the culture, agile reforms should be gradual.[213] Whatever the solution, the important thing is that people are the answer: procurement personnel making decisions and implementing policy on a daily basis will make or break agile reforms. Better regulations, no matter how well-worded, cannot do that.

### *C. To the Extent That Federal Procurement Law and Regulations Are To Blame, There Are Several Reforms That May Help*

"[I]t is tempting," Abraham Maslow quipped, "if the only tool you have is a hammer, to treat everything as if it were a nail."[214] Lawyers are susceptible to the same sort of category error, but laws are our hammers. We rarely see a problem that cannot be solved with a new or improved law or regulation.

Yet the reluctance to embrace agile is not mainly a legal problem. As described in the previous section, other forces are at work—such as

207. *See supra* notes 145–146 and accompanying text.

208. LAPHAM ET AL., *supra* note 78, at 49.

209. *See supra* note 189.

210. LAPHAM ET AL., *supra* note 78, at 11.

211. *See, e.g.*, Benjamin J. Balter, *Toward a More Agile Government: The Case for Rebooting Federal IT Procurement*, 41 PUB. CONT. L.J. 149, 168–69 (2011) (recommending additional training for contracting officers and other procurement professionals); NATIONAL RESEARCH COUNCIL, *supra* note 42, at 40–41 (lamenting that the Defense Acquisition University lacks "a comprehensive program to teach IT program management or IT test and evaluation").

212. LAPHAM ET AL., *supra* note 78, at 21.

213. *Id.* at 43 (describing a process for developing an agile acquisitions culture in the DoD).

214. ABRAHAM H. MASLOW, THE PSYCHOLOGY OF SCIENCE: A RECONNAISSANCE (1966).

culture, training, and inertia—and are much more important. Nevertheless certain legal or regulatory reforms may help to a degree, and we turn to those now.

In a passage in his book on the French Revolution, British philosopher and MP Edmund Burke contrasts easy and hard reforms. Easy reforms, he argues, can be made by mobs just well as by parliaments.[215] He continues:

> The shallowest undertaking the rudest hand is more than equal to that task. Rage and [f]renzy will pull down more in half an hour, than prudence deliberation and foresight can build up in an hundred years. The errors and defects of old establishments are visible and palpable. It calls for little ability to point them out. . . . To make every thing the reverse of what they have been is quite as easy as to destroy.[216]

This he contrasts with true progress, which is much harder won: "At once to preserve and to reform is quite another thing."[217]

This passage reminds us of the law of unintended consequences and that reforms should be made deliberately; reform and progress are not the same. We should be mindful not only that acquisition has undergone much reform in the past 50 years (and not all for the better)[218] and of the defects with cyber procurement, but also that there is much that is right about our system; some maintain the United States' acquisition system is the "envy of the world."[219] Notwithstanding what seem like serious defects with software procurement catalogued above

---

215. EDMUND BURKE, REFLECTIONS ON THE REVOLUTION IN FRANCE 247 (2d ed. 1790).

216. *Id.*

217. *Id.* He elaborates:

> When the useful parts of an old establishment are kept, and what is superadded is to be fitted to what is retained, a vigorous mind, steady persevering attention, various powers of comparison and combination, and the resources of an understanding fruitful in expedients are to be exercised; they are to be exercised in continued conflict with the combined force of opposite vices; with the obstinacy that rejects all improvement, and the levity that is fatigued and disgusted with everything of which it is in possession.

*Id.* at 247–48.

218. *The Department of Defense at High Risk: The Recommendations of the Chief Management Officer on Acquisition Reform and Related High Risk Areas*, *Report by the H. Comm. on Armed Services*, 111th Cong. 111–52 (2009) (describing 130 studies on acquisition processes since World War II and a near constant state of change to statute and regulations).

219. *See, e.g.*, *Politicizing Procurement: Will President Obama's Proposal Curb Free Speech and Hurt Small Business*?, *Joint Hearing Before the H. Comm. on Small Business and H. Comm. on Oversight and Government Reform*, 112th Cong. (May 12, 2011) (testimony of Daniel I. Gordon, Office of Management and Budget Office of Federal Procurement Policy, stating that the United States' acquisition system is the "envy of the world").

and a promising solution, any reforms should be made with due care. Thus, this paper returns to Burke's notion of genuine progress and the tradeoffs that come with the procurement reforms in the closing section.

Having made an extended disclaimer about hasty or careless reforms, three suggestions seem appropriate. First, we should consider a new process for IT that works outside the FAR. Second, we ought to consider eliminating or amending regulations that are inconsistent with agile. Third, Congress ought to reduce scrutiny over IT to facilitate agile development.

The FAR spans over 2,000 pages.[220] Some argue this complexity entails excessive transaction costs,[221] discourages the best in the private sector from competing,[222] and—most importantly here—is incompatible with agile.[223] Not all federal contracting dollars flow through the FAR,[224] so one option would be to carve out an exception for IT acquisitions.[225] Cooperative research and development agreements,[226] or the DoD's authority to enter into what are called "other transactions" for certain research projects,[227] may serve as models. Adapting the FAR and the myriad sub-regulations and culture implementing it may be impossible. Notwithstanding the lengthy Burke quote, good authority from an even older source holds that sometimes it is preferable to pour new wine into new bottles, else the

220. While this page count is considerable, it still pales in comparison to the Internal Revenue Service code, which doubled in size from 2003 to 2011, reaching 3.8 million words or 73,954 pages. *Companies and the State*, ECONOMIST (SPECIAL REPORT), Feb. 22, 2014, at 14 (giving word count and describing the influence of corporate lobbies on the growth in the IRS regulations); WOLTERS KLUWER, FEDERAL TAX LAW KEEPS ADDING UP (2013), http://www.cch.com/TaxLawPileUp.pdf (giving page count for the 2013 CCH STANDARD FEDERAL TAX REPORTER).

221. *See Challenges to Doing Business with the Department of Defense: Findings of the Panel on Business Challenges in the Defense Industry, H. Comm. on Armed Services* 112th Cong. (Mar. 19, 2012) (describing the high cost associated with contracting or otherwise doing business with the federal government, prepared by the Congressional Research Service, et al.).

222. *See, e.g.*, Johnson & Reed, *supra* note 47.

223. *See* Balter, *supra* note 211, at 165–66 (arguing a preference for competition over quality, long lead times, and stable requirements make the current system incompatible with agile).

224. CIBINIC ET AL., *supra* note 118, at 14–25 (explaining that the government engages a variety of non-FAR contractual arrangements).

225. DEFENSE SCIENCE BOARD REPORT, *supra* note 25, at 35–36 (quoting Secretary Gates's article, *supra* note 45, recommending that exceptions be carved out for warfighters' critical needs).

226. 15 U.S.C. § 3710a (2013) (authorizing directors of federal laboratories to enter CRADAs).

227. 10 U.S.C. § 2371(a) (2013) (granting DoD this authority for prototyping projects).

new wine burst the old bottles.[228] That is, it may be time to write a new IT-acquisition regulation uncontaminated by its predecessor.

If carving out an exception for IT proves untenable, we ought to consider revising acquisition laws and regulations to make them more compatible with agile. To take but one example, Lapham notes that a "particular sticking point" is that the DoD 5000 series regulations require large capstone events such as Critical Design Review.[229] Although there are workarounds, ideally regulations would be written without any lingering bias toward waterfall.[230] And this is not the only conflict between the regulations and agile methods.[231] If the DoD is to adopt agile, its regulations ought to be consistent with that aim.

Third, Congress ought to consider limiting its strict oversight of DoD IT acquisitions.[232] This would runs contrary to recent practice because starting in 2007 Congress increased oversight to "unprecedented levels."[233] This includes annual reports to Congress containing schedules with milestones, implementation schedules, life-cycles cost estimates, and key performance parameters summaries,[234]

---

228. *See* Matthew 9:14–17 (King James).

229. LAPHAM ET AL., *supra note* 78, at 11; *see also* DoDI 5000.02, Enclosure 2, ¶ 6.c.(6) (mandating critical design reviews and several other capstone events).

230. *Id.* at 13 (explaining that experienced contractors have accommodated the government and compromised with interim design reviews, which are more compatible with agile).

231. *Id.* at 12 (describing metrics and "granularity of estimates and task detail" requirements that are a poor fit for agile); LAPHAM, *supra* note 53, at 3 (explaining at the FAR and other acquisition regulations are cumbersome because they were written during the Cold War when the nation was not engaged in "dynamic warfighting" as it is today). Lapham. shared an anecdote that captures how just much red tape can encumber software development:

> If the government got a requirement to take a simple Hypertext PreProcessor (PHP)/mySQL-based forum type website that already exists in the .com and simply move it to the .mil, it could take *$3–5 million and a year to complete*. This would include, but not be limited to, documenting a new start, conducting a capabilities assessment, assigning a program manager, finding a host, doing the justification and approval, establishing contracts, getting the vendor and "approved" system for billing, briefing the required oversight groups, and so forth. If this type of requirement occurred within a commercial environment, it would take about *two hours and less than $1,000*.

*Id.* at 6 (emphasis added).

232. Congress has imposed a number of "legislative impediments" to agile reforms. For example, "the total dollar thresholds for designating oversight levels for IT programs are significantly lower than those used for weapons systems (by a factor of five). This results in a dichotomy in which an IT system with a development and deployment cost of $126 million over its life cycle has highly centralized oversight, while a weapons system counterpart at the same dollar level can be decentralized at the program executive officer level." *See* NATIONAL RESEARCH COUNCIL, *supra* note 42, at 44 (citation omitted).

233. DEFENSE SCIENCE BOARD REPORT, *supra* note 25, at 45–46.

234. *Id*. at 45; 10 U.S.C. § 2445C (2013) (requiring reports listed above commencing January 1, 2008).

as well as "Nunn-McCurdy-like reporting,"[235] whereby IT programs are judged using a baseline and "[a]ny change in cost, schedule, or performance that exceed[s] predefined limits will be associated with a significant or critical change" and "trigger[s] a report to Congress."[236] Such rigid reporting requirements resemble waterfall, trickle down to individual contracts, and make nominally agile efforts function like pseudo-waterfall. This is counterproductive, and comes at the same time Congress is demanding greater use of agile.[237] It is as if Congress were hitting the gas and slamming on the brakes at the same time. If it is serious about wanting agile to succeed, it must cut the red tape.[238]

---

235. This refers to the Nunn–McCurdy Amendment to the National Defense Authorization Act of 1983, which requires special reporting to Congress if a weapon system's cost per unit exceeds 15% of the original estimate and the cancelation if it exceeds 25%. *See* MOSHE SCHWARTZ, CONGRESSIONAL RESEARCH SERVICE, R41293, THE NUNN-MCCURDY ACT: BACKGROUND, ANALYSIS, AND ISSUES FOR CONGRESS 1–2 (2010); 10 U.S.C. § 2433 (2013) (codifying the Nunn–McCurdy Act).

236. DEFENSE SCIENCE BOARD REPORT, *supra* note 25, at 45–46 (describing several other reporting and oversight requirements under 10 U.S.C. § 2445C).

237. *See* NDAA for Fiscal Year 2010, Pub. L. No. 111–84, § 804, 123 Stat. 2190, 2402–03 (2009) (mandating agile for IT acquisitions).

238. This is, of course, an oversimplification. Detailing a cooperative relationship between the executive and legislative branches could be a paper unto itself. So this footnote attempts only to sketch what such a relationship might look like. It proceeds in three parts: first, it describes the constitutional oversight duties and powers; second, it notes the inherent tension between oversight and managerial flexibility; third, it offers some thoughts about squaring this circle.

Congress has a constitutional duty of oversight. *See* Watkins v. United States, 354 U.S. 178, 187 (1957) (explaining that the investigative power "is inherent in the legislative process"); Barenblatt v. United States, 360 U.S. 109, 111 (1959) (holding that "the scope of the power of inquiry, in short, is as penetrating as the potential power to enact and appropriate under the Constitution"). Congress has several tools at its disposal, including powers to subpoena, hold hearings, depose, grant immunity, hold in contempt, and bring suit. *See* MORTON ROSENBERG, INVESTIGATIVE OVERSIGHT: AN INTRODUCTION TO THE LAW, PRACTICE AND PROCEDURE OF CONGRESSIONAL INQUIRY 7–15 (2003); MARTIN O. JAMES, CONGRESSIONAL OVERSIGHT 32–37 (2002); JAMES HAMILTON, THE POWER TO PROBE: A STUDY OF CONGRESSIONAL INVESTIGATIONS 56–100 (1976). *Contra* LANCE COLE & STANLEY M. BRAND, CONGRESSIONAL INVESTIGATIONS AND OVERSIGHT: CASE STUDIES AND ANALYSIS 80–82 (2011) (recounting Supreme Court's limitations on congressional investigations following the "excesses" of the 1950s). This duty is heightened for defense expenditures for two reasons. First, the military constitutes the largest category of discretionary spending, and thus implicates Congress's duty to oversee the money it spends. *See* U.S. CONST. art. I, § 9, cl. 7 (providing "[n]o money shall be drawn from the Treasury" except by appropriations bills, establishing the power of the purse); *Barenblatt*, 360 U.S. at 111 (linking the breadth and depth of oversight powers to Congress's appropriation authority). Second, in addition to the power of the purse, the Constitution grants Congress an important role in the exercise of military powers. *See* U.S. CONST. art. I, § 8 (granting Congress power to "declare war," "raise and support armies," "provide and maintain a Navy," "make Rules for the Government and Regulation of the land and naval Forces," mobilize state militias, and "provide for organizing, arming, and disciplining" those state militias). This was by design. Having granted greater military powers to the federal government than existed under the Articles of Confederation, the framers "split these powers between the legislature and the executive" to

Though it may be counterintuitive, granting the DoD more flexibility to apply agile methods may well produce better results than would more waterfall-type scrutiny from Congress.

## CONCLUSION

Returning to where this paper started, the DoD desperately needs to do IT acquisition faster in order to do its job. Yet it has been slow to

---

ensure that these powers were not abused. *See* AKHIL REED AMAR, AMERICA'S CONSTITUTION: A BIOGRAPHY 114–19 (2005). Foremost among these safeguards was that military appropriations would last for no more than two years, and that Congress was thereby to keep a watchful eye on the danger to liberty that standing armies pose. *See generally* THE FOUNDERS' CONSTITUTION, Vol. 3, 122–66 (Phillip B. Kurland & Ralph Lerner eds., 1987) (assembling the framers' writings on the dangers of standing army and the protections afforded by Art. 1, § 8, cl. 11). In short, Congress must oversee military expenditures both because they are costly and because they are martial—both of which implicate important congressional roles under the Constitution. Such long-standing roles should not be taken lightly merely to expedite software development.

Yet congressional oversight is not free. *See* JOEL D. ABERBACH, KEEPING A WATCHFUL EYE: THE POLITICS OF CONGRESSIONAL OVERSIGHT 212–13 (1990) (describing the cost-benefit tradeoff that comes with any system of oversight); Kathleen Bawn, *Choosing Strategies to Control the Bureaucracy: Statutory Constraints, Oversight, and the Committee System*, 13 J.L. ECON. & ORG. 101, 105–06 (1997) (arguing for the optimal amount of congressional oversight in terms of political costs and benefits). Perhaps oversight should be balanced against "managerial flexibility." *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-05-117SP, PERFORMANCE BUDGETING: EFFORTS TO RESTRUCTURE BUDGETS TO BETTER ALIGN RESOURCES WITH PERFORMANCE 4–8, 13–14 (2005) (recognizing the tradeoffs between "managerial flexibility" and "congressional control"). Congress should never forsake its constitutionally mandated oversight duties, but it should nevertheless exercise *prudence*—lest micromanagement come at the expense of the flexibility necessary to the proper functioning of the executive agencies—in its exercise of those duties. "One basic issue cuts across most of the problems," Bernard Rosen explains, is "how to allow maximum possible independence while assuring adequate accountability." BERNARD ROSEN, HOLDING GOVERNMENT BUREAUCRACIES ACCOUNTABLE 54–56 (3rd ed. 1998).

It seems any viable executive-legislative relationship would exhibit at least three features. First, government personnel—whether employees or contractors—ought to be given "the legal, fiscal, and political independence" in order "to gain freedom from hierarchical control . . . in such matters as setting intermediate goals, establishing and applying standards," etc. ROSEN, *supra*, at 54 (summarizing Harvey Mansfield, *Independence and Accountability for Federal Contractors and Grantees*, *in* THE NEW POLITICAL ECONOMY (Bruce L.R. Smith ed., 1975)). That would mean less congressional scrutiny of milestones and the like, which are the bane of agile. Second, perhaps Congress ought to focus more on policy and less on management. Consultant Peter Drucker long counseled that elected officials are incapable of effective management, and ought to focus instead on policy. *See* PETER DRUCKER, THE AGE OF DISCONTINUITY 219–20 (1969). Following Drucker, perhaps Congress ought to operate at a strategic level and leave day-to-day tactical decisions to agency managers. Third, Congress would do well to constrain its oversight activities in order maximize their efficacy because a recent study suggests that less is more. Counterintuitively, increasing the number of committees "monitoring and potentially directing agency policymaking," lessens its influence and "undercut[s] the ability of Congress to respond collectively to the actions of the presidency or the bureaucracy." *See* Joshua D. Clinton, David E. Lewis & Jennifer L. Selin, *Influencing the Bureaucracy: The Irony of Congressional Oversight*, 57 AM. J. OF POL. SCI. 1, 2 (2013). Of course, much more could be written, but hopefully this provides a basic outline of how a healthy executive-legislative relationship might work.

adopt the agile reforms that have swept across the private industry. The previous section reviewed some regulatory obstacles, but none of those preclude agile.[239] Instead, the problem is that although laws and regulations use the jargon, "agile" acquisition is a misnomer as the DoD is stuck in the past, using methods discredited decades ago. There are regulatory obstacles, but the problem is mainly cultural.

Returning to Burke,[240] reforms can be harmful and progress does not come easily. We ought to take care before too hastily changing to a system that, all things considered, works fairly well—with the notable exception of cyber procurement. We should be wary of the inevitable tradeoffs.[241] Transparency is first among these. With agile we lose the top-down controls waterfall afforded, and may thereby lose some transparency. Yet that loss is not without recompense, and we may gain more than we lose.

Some argue that far from diminishing transparency, agile increases it. That is, while waterfall gives the false impression of transparency, agile delivers the real thing. Waterfall measures success against a standard established before development started; agile updates those standards in real-time, as end users provide feedback on each new iteration. Genuine transparency, the argument goes, is what makes agile both painful to adopt and worthwhile.[242]

Burke would counsel that when it comes to reforms, like Hippocrates, our watchword ought to be "first, do no harm." Yet even if agile resulted in lost transparency, it may still be worth the price. After all, a pristine system is not free; we pay not only in terms of formal controls, but also opportunity cost. At some point, surely value outweighs transparency. As described above,[243] the DoD has reached that point. It pays far too much for software that takes too long to develop and under-delivers. The time has come for agile reform.[244]

---

239. *See supra* note 189 (citing several studies indicating that federal procurement law and regulations do not preclude agile software development).

240. *See supra* notes 215–217 and accompanying text.

241. *See generally* Steven L. Schooner, *Desiderata: Objectives For a System of Government Contract Law*, 2 PUB. PROC. L. REV. 103, 103–09 (2002) (describing tradeoffs in public procurement policy among principles of competition, integrity, transparency, efficiency, customer satisfaction, best value, wealth distribution, risk avoidance, and uniformity).

242. I am indebted to Mr. Mark Schwartz, Chief Information Officer at United States Citizenship and Immigration Services (USCIS), who read an earlier version of this paper, for this insight.

243. *See* Sections II.B and II.C, *supra*.

244. If, as suggested above, *supra* note 242, and accompanying text, transparency isn't lost in the bargain, so much the better. It might be that agile increases *genuine* transparency. If so, agile

Whatever its effect on transparency, agile is an idea whose time has come. The DoD and Congress should dispense with rhetoric and develop a culture and regulatory framework consistent with the agile methods. That will not be easy.

Another challenge is the tension between agile and cybersecurity.[245] This paper has dwelt primarily on the need for timelier solutions to the DoD's needs because an acquisition cycle fast enough to keep up with the technology's rapid growth is essential to meeting those needs. But speed is not everything. Sometimes secure systems may come at the expense of speed, cost, or quality; a system that is late, costly, or ineffective may be preferable to one that is unsecure. Harnessing agile's advantages while also recognizing and compensating for its disadvantages will not be easy.[246]

Genuine agile reforms may not be easy, but they are urgent. Returning to the dangers catalogued at the outset,[247] cyber warfare presents the DoD with unprecedented challenges—especially given

---

software development would not only be cheaper, faster, and of better quality, it might also *increase*, not decrease, the integrity of our procurement system.

245. The tension between any agile methods or any form of rapid development methods and developing secure systems is well documented. *See, e.g.*, Steffen Bartsch, *Practitioners' Perspectives on Security in Agile Development*, Sixth International Conference on Availability, Reliability and Security, IEEE CONF. PUB. 479–84 (2011) (summarizing several studies on the tension between agile and cybersecurity).

246. Some argue that agile can be adapted to security or that they are not mutually exclusive. *See, e.g.*, SIMON BROWN, SOFTWARE ARCHITECTURE FOR DEVELOPERS (2013) (arguing there is no conflict between agile and architecture); Stephany Bellomo & Carol Woody, DOD INFORMATION ASSURANCE AND AGILE: CHALLENGES AND RECOMMENDATIONS GATHERED THROUGH INTERVIEWS WITH AGILE PROGRAM MANAGERS AND DOD ACCREDITATION REVIEWERS 1–2, 15 (2012) (suggesting agile is a net benefit to security as "shorter iterations make problems visible sooner so problems can be fixed earlier"); Deborah L. Farroha & Bassam S. Farroha, *Agile Development for System of Systems: Cyber Security Integration into Information Repositories Architecture*, 2011 Systems Conference IEEE CONF. PUB. (2011) (advocating a systems architecture that both utilizes agile methods and ensures security); Nancy R. Mead, et al., Venkatesh Viswanathan & Deepa Padmanabhan, *Incorporating Security Requirements Engineering into the Dynamic Systems Development Method*, Annual IEEE International Computer Software and Applications Conference, IEEE CONF. PUB. 949–54 (2011) (attempting to reconcile agile with security); Hossein Keramati & Seyed-Hassan Mirian-Hosseinabadi, *Integrating Software Development Security Activities with Agile Methodologies*, IEEE/ACS International Conference on Computer Systems and Applications IEEE CONF. PUB. 749–54 (2008) (attempting to reconcile agile and security); Mikko Siponen, et al., *Integrating Security into Agile Development Methods*, Proceedings of the 38th Hawaii International Conference on System Sciences, IEEE CONF. PUB. 1–7 (2005) (acknowledging conflict between secure and agile software development and suggesting how to harmonize the two); Konstantin Beznosov & Philippe Kruchten, *Towards Agile Security Assurance*, *in* NSPW '04: PROCEEDINGS OF THE 2004 NEW SECURITY PARADIGMS WORKSHOP 47–54 (ACM 2004) (identifying four security assurance methods, arguing that two of them clash with agile, and suggesting "ways of alleviating the conflict").

247. *See supra* Sections II.A and II.B.

that 90% of its weapons systems' functionality depends on software.[248] And the DoD lacks the tools to defend itself or to fight in the cyber domain because its IT-acquisition process is far too slow to keep pace with technological growth.[249] Fortunately, the arsenal of democracy[250] has provided a solution in the form of the agile software-development method. It's time for DoD IT acquisitions to do and to be agile, and not just rhetorically.

248. *See supra* note 25.
249. *See supra* Section II.C.
250. *See supra* note 3.