VIRGINIA JOURNAL OF
LAW & TECHNOLOGY

VOLUME 29 SYMPOSIUM 2026 NUMBER 2

PROSPECTING FOR PROGRESS

Andrea M. Matwyshyn[*]

[*] Andrea M. Matwyshyn is a Professor of Law and Engineering Policy at Penn State Dickinson Law and a Professor in SEDI at Penn State Engineering. She is the Founding Director of the Penn State Policy Innovation Lab of Tomorrow (PILOT).

TABLE OF CONTENTS

[W]e must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military-industrial complex. . . . We must never let the weight of this combination endanger our liberties or democratic processes.
– President Dwight D. Eisenhower[1]

This is our world now. The world of the electron and the switch, the beauty of the baud.
– Agent Bob[2]

INTRODUCTION

GOVERNMENT technology procurement has been having a rough time lately. In an attempt to leverage the benefits of new technologies, governments have experimentally adopted a plethora of new tools — particularly various forms (of the technologies we call) artificial intelligence ("AI"). But, as the results of these early adoptions arrive, the outcomes have sometimes ended in irreparable harms and counterproductive effects. In 2024, the State of Michigan settled allegations that it had procured an inadequately tested, flawed predictive analytics tool, a tool "that operated without human supervision and had an error rate as high as 93%";[3] the tool had falsely accused over 40,000 Michiganders of defrauding the state of unemployment benefits between 2015 and 2017.[4] In Arkansas, an AI tool procured by the Department of

[1] *President Dwight D. Eisenhower's Farewell Address (1961)*, NAT'L ARCHIVES (last reviewed July 15, 2024), https://www.archives.gov/milestone-documents/president-dwight-d-eisenhowers-farewell-address [https://perma.cc/F94Z-Z64Z].

[2] HACKERS (United Artists 1995) (quoting Loyd Blankenship (a.k.a. The Mentor), *The Hacker's Manifesto* (Jan. 8, 1986), available at https://www.mithral.com/~beberg/manifesto.html [https://perma.cc/J37F-TRKG]).

[3] Adrienne Roberts, *Thousands of Michigan Residents Wrongly Accused of Fraud to Get $1,600 Checks*, DETROIT FREE PRESS (Jan. 2, 2024), https://www.freep.com/story/money/business/michigan/2024/01/02/michigan-midas-unemployment-false-fraud-settlement-money/72084899007/ [https://perma.cc/2FAJ-EN6W]; *see also* Thomas Claburn, *Fraud Detection System with 93% Failure Rate Gets IT Companies Sued*, REGISTER (Mar. 8, 2017), https://www.theregister.com/2017/03/08/fraud_detection_system_with_93_failure_rate_gets_it_companies_sued/ [https://perma.cc/96UL-5SY8].

[4] *See* David Eggert, *State Apologizes for Fraud Fiasco, Wants to Reduce Penalties*, ASSOCIATED PRESS (Jan. 28, 2017), https://apnews.com/united-states-congress-c0e2346e85854a5b827ca42653c1fb40 [https://perma.cc/JJ6T-WYLX] ("Michigan's embattled unemployment benefits office apologized for the fiasco that led at least 20,000 people to be falsely accused of defrauding a system that provides the jobless with temporary financial assistance.").

Human Services resulted in adverse consequences for nearly half of the state's Medicaid population until its use was enjoined by a federal court.[5] More recently, a different Arkansas procurement of an infrastructure update to its child welfare systems failed after two years of work.[6] In Maryland, an AI gun detection system procured for schools misidentified a tortilla chip bag as a weapon, leading to an unnecessary student encounter with the police,[7] and in Florida, a school went into lockdown when another AI system procured for a school misidentified a clarinet as a weapon.[8] A still different system procured in Tennessee failed to identify a weapon prior to a deadly school shooting.[9] In Pennsylvania, an AI tool procured by Allegheny County is currently under investigation by the Department of Justice for potential discrimination against parents with disabilities[10] in connection with removals of children from homes.[11] Meanwhile, in another part of the state, a vulnerable water system component procured by Aliquippa County Municipal Water Authority allowed for remote attackers to shut down a device that regulates water pressure at a pumping station.[12] On the federal level, the F-35 program

[5] Ark. Dep't Hum. Servs. v. Ledgerwood, 530 S.W.3d 336 (Ark. 2017).

[6] Tess Verbin, *Effort to Upgrade Arkansas Child Welfare Computer System Fails After Two Years*, MT. HOME OBSERVER (Sep. 9, 2025), https://mhobserver.com/effort-to-upgrade-arkansas-child-welfare-computer-system-fails-after-two-years/ [https://perma.cc/ZF4Y-XVDE].

[7] Kristen Griffith, *Baltimore County School's AI Gun Detection System Mistook a Bag of Chips for a Weapon*, THE BALTIMORE BANNER (Oct. 22, 2025), https://www.thebanner.com/education/k-12-schools/kenwood-high-school-omnilert-gun-chips-false-alarm-YJEL25XTVRBUDFDIJ7TEOBEKCY/ [https://perma.cc/U2U3-9TUZ].

[8] Joe Pring, *School Enters Lockdown After AI Mistakes Student's Clarinet for a Weapon*, DEXTERO (Dec. 13, 2025), https://www.dexerto.com/entertainment/school-enters-lockdown-after-ai-mistakes-students-clarinet-for-a-weapon-3293663/ [https://perma.cc/EV68-MU2E].

[9] Noor Al-Sibai, *School's $1 Million AI Gun Detection System Fails to Detect Weapon Before Fatal School Shooting*, FUTURISM (Jan. 24, 2025), https://futurism.com/the-byte/school-shooting-ai-gun-detection-failure [https://perma.cc/SX8K-DXEV].

[10] Sally Ho & Garance Burke, *Child Welfare Algorithm Faces Justice Department Scrutiny*, ASSOCIATED PRESS (Jan. 31, 2023), https://apnews.com/article/justice-scrutinizes-pittsburgh-child-welfare-ai-tool-4f61f45bfc3245fd2556e886c2da988b [https://perma.cc/TWY8-LYWT].

[11] Laurel-Ann Dooley, *Does Artificial Intelligence Discriminate in Child Neglect Case Assessments?*, ABA J. (Dec. 1, 2023) (describing Professor Robyn Powell's belief that the problem may lie in the particular data points used in screening, which arise from past cases; the screening tool generates a risk score that potentially includes criteria that are expressly disallowed by law and replicates existing problematic removals), https://www.abajournal.com/magazine/article/does-artificial-intelligence-discriminate-in-child-neglect-case-assessments.

[12] Associated Press, *Cyber Attack at Municipal Water Authority in Pennsylvania Prompts Renewed Cybersecurity Warnings*, WNEP 16 (Jan. 2, 2024),

has allegedly been plagued by uncorrected design flaws, security vulnerabilities, and unreliability issues,[13] and the procurement choice of multiple agencies in using the Solar Winds software reportedly led to the security compromise of about a dozen federal agencies (and approximately 100 companies) by attackers linked to foreign intelligence services.[14] Additional technology procurement disasters are unfortunately likely to be on the horizon, in light of staff shortages and security infrastructure elimination on the federal level[15] and budgetary struggles on the state level.[16] Yet, federal agencies were poised to spend over $3.3 billion on AI and related technologies in 2025, according to some analysts; but these analysts caution that project proposals often raised familiar categories of technology procurement concerns, including "boilerplate cybersecurity plans without addressing AI-specific risks[,]

https://www.wnep.com/article/news/state/water-authority-hacked-pennsylvania-cybersecurity-warnings-federal-security-officials/523-1b311bd6-5f7c-416e-ac80-975e1a1447e1. This cyber-attack also has concerning implications for the private sector, as many private entities seem to rely on the same vulnerable component as the public sector did. *See* Frank Bajak & Marc Levy, *Breeches by Iran-Affiliated Hackers Spanned Multiple U.S. States, Federal Agencies Say*, ASSOCIATED PRESS (Dec. 2, 2023), https://apnews.com/article/hackers-iran-israel-water-utilities-critical-infrastructure-cisa-554b2aa969c8220016ab2ef94bd7635b ("[O]ther industries outside water and water-treatment facilities use the same equipment . . . and [are] also potentially vulnerable."); Cybersecurity & Infrastructure Sec. Agency, *IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities*, Alert Code AA23-335A (Dec. 18, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a (warning of the broader effects of these attacks).

[13] Dan Grazier, *Uncorrected Design Flaws, Cyber-Vulnerabilities, and Unreliability Plague the F-35 Program*, PROJ. ON GOV'T OVERSIGHT (Mar. 24, 2020), https://www.pogo.org/analyses/uncorrected-design-flaws-cyber-vulnerabilities-and-unreliability-plague-the-f-35-program; Tony Capaccio, *Declassified Pentagon F-35 Study Details Reliability, Security Woes for America's Costliest Weapon*, SPOKESMAN REV. (Nov. 21, 2024), https://www.spokesman.com/stories/2024/nov/21/declassified-pentagon-f-35-study-details-reliabili/ [https://perma.cc/HLQ2-LZ6F].

[14] Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack*, NPR (Apr. 16, 2021), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack [https://perma.cc/TNL8-YMME].

[15] Nicole Sganga, *Cybersecurity Agency's Top Recruits Decimated by DOGE Cuts*, CBS NEWS (March 17, 2025), https://www.cbsnews.com/news/cybersecurity-agencys-top-recruits-doge-cuts/.

[16] *2024 Deloitte-NASCIO Survey Finds States Face Growing Cybersecurity Threats, Tight Budgets*, NAT'L ASS'N OF STATE CHIEF INFO. OFFICERS (Sept. 30, 2024), https://www.nascio.org/press-releases/2024-deloitte-nascio-survey-finds-states-face-growing-cybersecurity-threats-tight-budgets/ [https://perma.cc/S9YD-9CTW].

. . . governance language [that] is too generic, . . . [and e]thical AI policies [that] are copy-pasted . . . and don't explain how risk is managed."[17]

Internationally, the technology procurement prospects are no brighter. In Rotterdam, "[m]ore than 20,000 families were wrongly accused of childcare benefit fraud after a machine learning system was used to try to spot wrongdoing" leading to "[f]orced evictions, broken homes, and financial ruin . . . and the entire Dutch government resigned in response in January 2021."[18] In Australia, the so-called "robodebt scandal'[19] arose when a third party debt processor was procured to replace the formerly manual system of calculating overpayments and issuing debt notices to welfare recipients; the debt processor falsely accused members of the public of nonpayment of tax debt, leading to multiple suicides and a Royal Commission that referred a number of government employees for further investigation.[20] In the UK, a Post Office scandal involved a failed procurement where a contractor's purpose-built algorithm allegedly remotely modified accounting records of individual postmasters, resulting in over 900 wrongful accusations[21] and over 700 wrongful convictions of criminal fraud in what is viewed as "the wildest miscarriage of justice in UK history."[22]

[17] *AI Contracts and Federal Procurement: The $20 Billion Wave Contractors Are Missing*, U.S. FED. CONT. REGISTRATION (Aug. 8, 2025), https://blogs.usfcr.com/ai-contracts-federal-procurement.

[18] Matt Burgess, Evaline Schot & Gabriel Geiger, *This Algorithm Could Ruin Your Life*, WIRED (Mar. 6, 2023, 7:00 AM), https://www.wired.co.uk/article/welfare-algorithms-discrimination [https://perma.cc/247D-46US]. Wrongly accused targets expressed feelings of being gaslit and contemplating suicide, particularly after some people were wrongly accused multiple times by the algorithms. All 315 factors of the risk-scoring system were initially set to describe an imaginary person with "average" values in the data set. "They don't know me, I'm not a number. I'm a human being," A Rotterdam resident said. After two welfare fraud investigations, the resident became angry with the system. "They've only opposed me, [and] pulled me down to suicidal thoughts." Another individual stated that he "couldn't focus on anything else and didn't think he had a future. 'It got really difficult. I thought a lot about suicide, . . .'" *Id.*

[19] *See, e.g.*, Frances Mao, *Robodebt: Illegal Australian Welfare Hunt Drove People to Despair*, BBC (July 7, 2023), https://www.bbc.com/news/world-australia-66130105 [https://perma.cc/65V3-GUWT] ("[A]n illegal welfare hunt by the previous government made victims feel like criminals and caused suicides.").

[20] ROYAL COMM'N, INTO THE ROBODEBT SCHEME, REPORT, at iii (2023).

[21] *Post Office Horizon Scandal: Why Hundreds Were Wrongly Prosecuted*, BBC (Oct. 9, 2025), https://www.bbc.com/news/business-56718036 [https://perma.cc/537D-G9S9].

[22] Karl Flinders, *Post Office Horizon Scandal Explained: Everything you Need to Know*, COMPUT. WKLY. (Sept. 10, 2025), https://www.computerweekly.com/feature/Post-Office-Horizon-scandal-explained-everything-you-need-to-know [https://perma.cc/AJR9-X9DU]. Wrongly accused postmasters in some cases committed suicide under the strain of the adversarial attack on identity, and the formal inquiries and litigation continue two decades later to ascertain the full extent

As explained by Professor Christopher Yukins:

> Over the past several decades, the federal procurement system in the United States has grown remarkably . . . . Over that same period, the rules governing federal procurement have been buffeted by broad efforts at reform. At no point, however, have we ever had an overarching theory — a model or prism — through which to assess the procurement system or its reform. Agency theory provides one such theoretical model.[23]

But Yukins highlights that some issues exist "beyond what principal-agent theory can explain and thus makes it clear that other normative structures must be shaping the procurement system as well."[24] Responsively, in the context of trade secret concerns and procurement, Professor Elizabeth Rowe and a coauthor advocate that we "reorient the [procurement] analysis to an earlier time period — the point at which the government agency initially decides to purchase the software," explaining that "[c]ontracts can balance the competing interests of secrecy and disclosure, and contractual negotiations between government agencies and private vendors are the means for achieving such balance on a transaction-by-transaction basis."[25] Other legal scholars have argued in favor of explicitly crafting more robust procurement rules in connection

of the known software flaws and intentional ledger manipulations. Litigation continues two decades after the initial corruption of the postal ledgers by software. *Id.*; *see also* Sylvia Hui, *At Least 13 May Have Killed Themselves over UK's Post Office Wrongful Convictions Scandal*, AP NEWS (July 8, 2025), https://apnews.com/article/uk-post-office-scandal-suicide-horizon-software-70a6945a3acf945ea9d121425fdd028c [https://perma.cc/H8F2-L9FL].

[23] Christopher R. Yukins, *A Versatile Prism: Assessing Procurement Law Through the Principal-Agent Model*, 40 PUB. CONT. L.J. 63, 63–64 (2010) ("Long established in economics and the other social sciences, the principal-agent model (agency theory) provides a model to explain successes (and failures) in organizational structures, and also to understand the procurement system and its rules. The theory builds upon the classic principal-agent model.").

[24] "For example, although most such rules constrain conflicts of interest in acquisition decisions and thus fall squarely within the four corners of agency theory, there are other conflict-of-interest rules that deal with officials' actions after government employment, which do not seem meant to protect acquisition decisions directly. If agency theory explains conflict-of-interest rules that constrain purchasing decisions, that theory logically cannot explain rules that govern behavior after an official has left her/his post and can no longer make purchases on the principal's behalf. To explain these post-employment rules, therefore, either we must stretch the principal-agent model (sometimes beyond all recognition) or we must consider other norms and other models to fully explain other pieces of an enormously complex procurement system." *Id.* at 82.

[25] Elizabeth A. Rowe & Nyja Prior, *Procuring Algorithmic Transparency*, 74 ALA. L. REV. 303, 308 (2022).

with computer security/cybersecurity baselines, partially in furtherance of nudging the private sector toward stronger security practices.[26] This author has also proposed the creation of a new agency, a Bureau of Technology Safety, a portion of whose duties would include assisting other agencies in "troubleshooting" their complex technology procurement needs and emergencies and assisting them with forward looking threat modeling and technology procurement planning.[27]

This Essay expands on foundational work by these and other scholars[28] to offer a novel conceptual model for the future of government technology procurement — a Procurement in Nested[29] Technologies ("PINT") model.[30] The key differences of the PINT model of procurement are twofold. First, it recognizes the erosion of the traditional framing of "procurement" that views it as being synonymous with "acquisition." Instead, it adopts an approach informed by theory of computer security and developmental psychology. Recognizing a trajectory in procurement toward a model of human-machine

[26] Andrea M. Matwyshyn, *Cyber!*, 2017 B.Y.U. L. REV. 1109, 1192 (2017) [hereinafter *Cyber!*] ("Vendors that fail to patch vulnerabilities on a timely basis should be deemed in material breach of agreements and blacklisted from procurement vendor lists. Because of the purchasing power of the U.S. government and public companies in particular, this approach, which combines better vulnerability assessments and blacklists, would trigger significant security improvements in supply chain integrity in both the public and private sectors expeditiously."); Andrea M. Matwyshyn, *Cyber Harder*, 24 B.U. J. SCI. & TECH. L. 450, 492 (2018) ("Demands for security improvements from public companies will create network effects of security improvements in their vendors' conduct, as do the purchasing requirements of the U.S. government. Hence, this supply chain security monitoring would stimulate significant improvements in supply chain integrity in both the private and public sector").

[27] Andrea M. Matwyshyn, *Exploit Machina*, 59 U.C. DAVIS L. REV. 1635 (2026).

[28] *See also, e.g.*, Ryan Calo & Danielle Keats Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 EMORY L.J. 797, 797 (2021) (arguing that "[a]utomation abdicates the expertise and nimbleness that justify the administrative state, undermining the very case for the existence and authority of agencies"); Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 GEO L.J. 1147 (2017).

[29] Nested models are common both to psychology and computing. *See, e.g.*, *JavaScript 08: Advanced Objects in JavaScript: Nested Structures and Data Handling*, MEDIUM (Oct. 30, 2024) https://javascript.plainenglish.io/javascript-08-advanced-objects-in-javascript-nested-structures-and-data-handling-52caa4d01b55.

[30] The nested model borrows structures and insights from the world of Urie Bronfenbrenner. See generally, URIE BRONFENBRENNER, THE ECOLOGY OF HUMAN DEVELOPMENT: EXPERIMENTS BY NATURE AND DESIGN (Harv. Univ. Press, 1981); Urie Bronfenbrenner, *Toward an Experimental Ecology of Human Development*, 32 AM. PSYCH. 513, 513–31 (1977).

symbiosis,[31] it explains that the reciprocal security vulnerability[32] of public and private sector technologies (and social systems) now require heightened considerations of resilience. Therefore, the PINT model consciously centers the principles of social resilience and technology progress[33] as public policy objectives. Second, it reframes procurement from a linear, static series of government acquisitions into a nonlinear, dynamic process. In this way, PINT recognizes the fundamental differences between the role of the private sector and the public sector in society, despite their growing reciprocal vulnerability. As such, it replaces one-size-fits-all discussions of procurement "efficiency" with more concrete determinations of mission efficacy in context, allowing for more precise assessments of movement toward long term progress objectives. In other words, PINT facilitates future-looking assessments that include audit and self-improvement by design. Leveraging the strengths of our federalist model of government, PINT allows for differentiated evolution of public and private sector governance, while maintaining shared national security and resilience objectives. Section I introduces reasons for considering a new conceptual model for technology procurement. Section II introduces the nested PINT model.

I. WHY WE NEED A NEW CONCEPTUAL MODEL FOR TECHNOLOGY PROCUREMENT

Akin to, and largely responsible for the sweeping changes in our industrial-military posture, has been the technological revolution during recent decades.
– President Dwight D. Eisenhower[34]

Discussions of procurement have generally viewed the process to involve the acquisition of particular products and services by the government for government use. However, because of the evolution of both procurement practices and the computer security risks of modern technologies, traditional frameworks may no longer hold their former explanatory power. As we move toward models of machine-human symbiosis in technology operations in both the public and private sector,

[31] The first articulation of a model of human-machine symbiosis is usually attributed to J.C.R. Licklider. *See* J.C.R. LICKLIDER, MAN–COMPUTER SYMBIOSIS, HFE-1 IRE TRANSACTIONS ON HUMAN FACTORS IN ELECTRONICS 4 (March 1960) http://memex.org/licklider.pdf.

[32] Procurement as used herein is not synonymous with "acquisition," thereby breaking with traditional scholarship on point. For a discussion of the need for a distinction between procurement and acquisition, see *infra* Section I.

[33] *See* U.S. CONST. art. I, § 8.

[34] *Eisenhower's Farewell Address*, *supra* note 1.

a reconsideration of traditional technology procurement models is timely.

A. The Evolution of Procurement Law

As explained in 48 C.F.R. § 1.102 "[t]he vision for the Federal Acquisition System is to deliver on a timely basis the best value product or service to the customer, while maintaining the public's trust and fulfilling public policy objectives."[35] But, as explained by John S. Pachter:

> The [Federal Acquisition Regulation (FAR)] states that "procurement" is synonymous with acquisition. Acquisition, in turn, means the acquiring by contract with appropriated funds of supplies or services (including construction) by and for the use of the Federal Government . . . ."In short, a procurement contract must involve (1) acquisition of supplies or services "by and for the use of the Federal Government" and (2) the use of appropriated funds. Yet, in at least two . . . decisions, the courts, deferring to DoD, ignored the FAR definition and held that a

[35] 48 C.F.R. § 1.102(a). Participants in the acquisition process should work together as a team and should be empowered to make decisions within their area of responsibility.

(b) The Federal Acquisition System will—

(1) Satisfy the customer in terms of cost, quality, and timeliness of the delivered product or service by, for example—

(i) Maximizing the use of commercial products and commercial services;

(ii) Using contractors who have a track record of successful past performance or who demonstrate a current superior ability to perform; and

(iii) Promoting competition;

(2) Minimize administrative operating costs;

(3) Conduct business with integrity, fairness, and openness; and

(4) Fulfill public policy objectives.

(c) The Acquisition Team consists of all participants in Government acquisition including not only representatives of the technical, supply, and procurement communities but also the customers they serve, and the contractors who provide the products and services.

(d) The role of each member of the Acquisition Team is to exercise personal initiative and sound business judgment in providing the best value product or service to meet the customer's needs. In exercising initiative, Government members of the Acquisition Team may assume if a specific strategy, practice, policy or procedure is in the best interests of the Government and is not addressed in the FAR nor prohibited by law (statute or case law), Executive order or other regulation, that the strategy, practice, policy or procedure is a permissible exercise of authority.

48 C.F.R. § 1.102(b)–(d).

> contract was a procurement contract even though it met neither condition.[36]

In other words, as explained by legal experts on procurement, caselaw has already cast doubt on a traditional interpretation of the relevant statutes and explanatory FAR definitions,[37] seeming to create a space for categories of procurement that may not, strictly speaking, fall into the category of an "acquisition."

Congressional appropriations in practice[38] appear to demonstrate a similar drift. For example, in the Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, the breadth of forms of technology procurement Congress contemplated goes beyond a narrow view of goods and services "by and for the use of the Federal Government."[39] For example, the Act contemplates rapid prototyping of entirely new technologies,[40]

[36] John S. Pachter, *What Is a Procurement? And Why Can't DoD and the Courts Get It Straight?*, 34 PUB. CONT. L.J. 1, 2–3 (2004).

[37] *Id.* at 5–6 ("[T]he question whether a concession contract is a "procurement" contract came before the Supreme Court in National Park Hospitality Ass'n v. United States Department of the Interior on review of the D.C. Circuit's decision in Amfac Resorts, L.L.C. v. United States Department of the Interior The D.C. Circuit had ruled that contracts for concessions at national parks are not "procurement" contracts within the meaning of the Contract Disputes Act of 1978. That court held that concession contracts do not involve the purchase of goods and services by and for the Government, but instead authorize third parties to provide services to park area visitors[26] . . . [which] the Supreme Court dismissed the appeal for lack of ripeness.").

[38] Margaret E. McConnell, *The Process of Procuring Information Technology*, 25 PUB. CONT. L.J. 379, 380–81 (1996) (explaining that "[t]he traditional approach to public purchasing is well known to practitioners of public contract law"). McConnell goes on to describe the traditional approach to public purchasing as:

> [T]he process typically calls for prespecification of requirements (often with the weight to be given to each requirement in the vendor evaluation process), followed by objective selection of the proposal that best meets those requirements. To ensure objectivity, detailed rules have been generated to guide the process . . . . The procurement process focuses on controlling bias or favoritism in order to preserve free and open competition, thus seeking the lowest cost for taxpayers and fairness for vendors. . . . Procurement awards are usually based primarily on price (since lowest price is both an important criterion for selecting among bidders and perceived to be the objective). Awards are rarely determined by past performance (because measuring past performance would be subjective or create a bias against new contractors). The focus of procurement decision making is very much on one contract at a time.

[39] Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118–159, 138 Stat 1773 (2024), https://www.congress.gov/118/plaws/publ159/PLAW-118publ159.pdf.

[40] *Id.* "(b) ACQUISITION PATHWAYS.—The Under Secretary of Defense for Acquisition and Sustainment shall establish the following two acquisition pathways:

something that was successfully implemented in earlier generations of procurement to stimulate the creation of new techniques and tools in computer security.[41] It also contemplates workforce creation and technology training initiatives, reflecting the importance of human capital — what computer security professionals would call human factors — as key components of successful procurement strategy.[42] Yet again, these are appropriated initiatives that are not merely "pulling" products and services from the private sector; they are often consciously stimulating their creation where the market has failed to produce them. For example, private sector commercialization of the global positioning system,[43] semi-autonomous cars,[44] spreadsheets,[45] and the internet itself[46] would not exist in modern form without the funding that arose

(1) RAPID PROTOTYPING.—The rapid prototyping pathway shall provide for the use of innovative technologies to rapidly develop fieldable prototypes to demonstrate new capabilities and meet emerging military needs. The objective of an acquisition program or project under this pathway shall be to field a prototype that can be demonstrated in an operational environment and provide for a residual operational capability within five years of the development of an approved requirement.

(2) RAPID FIELDING.—The rapid fielding pathway shall provide for the use of proven technologies to field production quantities of new or upgraded systems with minimal development required. The objective of an acquisition program or project under this pathway shall be to begin production within six months and complete fielding within five years of the development of an approved requirement."

[41] The DARPA Cyber Fast Track ("CFT") was a highly successful initiative that reflects these broader procurement dynamics, only stimulating novel invention but also identifying with particularity economy-wide problems for correction through both private and public sector means. *See, e.g.*, Dennis Fisher, *Groundbreaking Cyber Fast Track Research Program Ending*, THREATPOST (Mar. 6, 2013) https://threatpost.com/groundbreaking-cyber-fast-track-research-program-ending-030613/77594/ ("The CFT program was designed to help deliver funding quickly for interesting security research proposals. . . . [T]he CFT program so far has received nearly 400 proposals and handed out grants to 101 of them . . . [The program manager also found] that by looking at the security advisories put out by security vendors themselves on their own products, he could identify that on average each month, about 28 percent of the vulnerabilities introduced are from defensive technologies.").

[42] Service Member Quality of Life Act, *supra* note 39. *See also, e.g.*, Title II, Subtitle A §§ 221–22, 236–38; Title XV, Subtitle D § 1531–34; Title XVI, Subtitle C § 1638; Title LXV § 6504.

[43] Christy Wyskiel, *The Academic Origins of Everyday Tech*, FAST CO. (Nov. 17, 2025), https://www.fastcompany.com/91443762/the-academic-origins-of-everyday-tech.

[44] *Id.*

[45] *Id.*

[46] ARPANET, DARPA (July 2020), https://www.darpa.mil/news/features/arpanet.

from government financial support and procurement processes,[47] frequently from the Defense Advanced Research Projects Administration (DARPA) and its predecessors.[48] These necessary and more expansive understandings of procurement arguably renew the intellectual space for a conversation around modernized theories and models of technology procurement.

These new types of procurement initiatives are potentially in part a response to historical critiques from procurement practitioners[49] and academics,[50] who flagged tensions that may arise between the cultural norms of older models of procurement and the realities of modern technology development.[51] In other words, this shift in procurement on the ground (and in the cloud) includes two key bi-directional dynamics: first, the need to address human elements of technology governance and the changing risk profile of modern technology; and second, to acknowledge more expressly the role that the government plays in pushing forward technology progress, not merely acquiring it.

As modern technologies introduce new categories of risk and exacerbate old categories, they present both challenges and opportunities for a new model for technology procurement policy that maps to the reality already emerging on the ground. Chief among these technological

[47] Indeed, according to some estimates, since 1980, federal dollars have stimulated the creation of over 17,000 small businesses and $1.9 trillion in financial output. Wyskiel, *supra* note 43.

[48] *See id.*

[49] *See* Margaret E. McConnell, *The Process of Procuring Information Technology*, 25 PUB. CONT. L.J. 379, 390–91 (1996).

[50] For example, in 1995, a Harvard University report "Information Technology and Government Procurement: Priorities for Reform," offered four recommendations for the future of technology procurement:

1. Distinguish[ing] between "commodities" (simple and well-known goods and services) and "noncommodities" (complex and novel goods and services) and design[ing] different procurement processes for each. . . .

2. Prepar[ing] for electronic markets and commerce, ... [including] developing[ing] electronic procurement aids . . . [and additional] post-audit controls. . . .

3. Support[ing] managerial discretion and organizational learning, ... [i]ncreas[ing] . . . the weight given to vendors' past performance . . . . [and e]stablish[ing] procurement guidelines to support the development of systems based on their evolution [and related initiatives] . . . .

4. Organiz[ing] around issues of [technology] . . . as much as [around] procurement per se.

McConnell, *supra* note 49, at 389 n.30 (citing Jerry Mechling, *Draft Report for the Program on Strategic Computing and Telecommunications in the Public Sector*, HARV. KENNEDY SCH. GOV'T 17–20 (1995)).

[51] Some authors have pointed to governmental "cultures" and norms pushing toward older models of development such as so-called "waterfall" processes of development; instead, these authors advocate stronger commitment to "agile" development models.

risk elements involves what legal scholars have called the "reciprocal security vulnerability" of the public and private sector.[52] This Essay builds on these critiques to argue that the challenges (and opportunities) of technology procurement warrant a shift toward a conceptual model closer to one of human-machine symbiosis.[53]

B. The Reciprocal Nature of Security Vulnerability: Lessons From Technology Procurement History

As explained by this author in previous work, the problem of reciprocal security vulnerability refers to the recognition "that corporate information security and national "cybersecurity" concerns are inextricable" because of their frequent shared reliance on the same technology tools, code libraries, and products and services.[54] Because vulnerability and potential exploitation arise wherever problematic lines of code exist, the practical realities of computer security mean that the same vulnerable code can be exploited simultaneously in both the public and private sectors.[55] As such, the traditional legal lines of segmentation between public and private sector governance, contractual relationships, agency law considerations and other dynamics are inexorably altered in a technology-reliant environment; computer security threats do not respect legal public-private boundaries (or the rules of procurement processes).[56]

The problems of reciprocal security vulnerability and their connection to procurement manifest across each of the three categories of computer security properties — confidentiality, integrity, and availability.[57]

1. Confidentiality

In computer security, confidentiality refers to "preserving authorized restrictions on information access and disclosure, including means for

[52] *Cyber!*, *supra* note 26, at 1109.

[53] *See* discussion *infra* Section I, Part C.

[54] *Cyber!*, *supra* note 26, at 1109.

[55] *Id.* at 1121–23, 1133–34.

[56] *Id.* at 1116–17, 1121. *See also* Kristen Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV.467 (2017).

[57] Jennifer Cawthra et al., *Data Integrity: Detecting and Responding to Ransomware and other Destructive*
Events, NAT'L CYBERSECURITY CTR. FOR EXCELLENCE (2020), https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html.

protecting personal privacy and proprietary information."[58] Consider, for example, a 2020 supply chain confidentiality compromise that led to irreparable harms — the compromise of multiple "U.S. government agencies, critical infrastructure entities, and private sector organizations by an advanced persistent threat [] actor."[59] A trusted[60] (private contractor) supplier, SolarWinds, experienced a "nefarious alteration of trusted software at its source."[61] The product in question, Orion, has been "described as a 'single pane of glass' that can monitor everything in a system,"[62] and some experts have called the compromise "unprecedented" because of "its capability to cause significant physical consequences."[63] According to facts presented in the (recently withdrawn) Securities and Exchange Commission (SEC) complaint filed against the company in 2023,[64] internal reports by employees[65] of

[58] *Id.*

[59] *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY CYBERSECURITY ADVISORY (revised Apr. 15, 2021) [hereinafter *Advanced Persistent Threat Compromise*], https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a; *see also* Associated Press, *SolarWinds Hack Got Emails of DHS Head and Other Top Officials*, NBC NEWS: NAT'L SEC. (Mar. 29, 2021, 11:15 AM), https://www.nbcnews.com/politics/national-security/solarwinds-hack-got-emails-dhs-head-other-top-officials-n1262329; Helen Warrell & Hannah Murphy, *What Do We Know About the SolarWinds Hack?*, FIN. TIMES (Dec. 14, 2020) ("According to its website, SolarWinds' clients include Microsoft, McDonald's, Lockheed Martin and Yahoo . . . ."), https://www.ft.com/content/3558b9b6-465f-4338-9d66-70b2fbe8f900.

[60] For a discussion of the critical role in legal analysis played by the computing theory distinctions between trusted and trustworthy versus trusted but untrustworthy suppliers, *see, e.g.*, Andrea M. Matwyshyn & Miranda K. Mowbray, *Fake*, 43 CARDOZO L. REV. 643, 700–08 (2022).

[61] Kim Zetter, *The Untold Story of the Boldest Supply-Chain Hack Ever*, WIRED (May 2, 2023, 6:00 AM), https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/; Saheed Oladimehi & Sean Michael Kerner, *SolarWinds Hack Explained: Everything You Need to Know*, TECHTARGET (Nov. 3, 2023), https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know. According to press reports, more than 30,000 public and private organizations used the Orion network management system. Because of its compromise, SolarWinds allegedly delivered the backdoor malware as an update to the Orion software; more than 18,000 SolarWinds customers reportedly installed the malicious updates. *Id.*

[62] Warrell & Murphy, *supra* note 59.

[63] Pam Baker, *The SolarWinds Hack Timeline: Who Knew What, and When?*, CSO (June 4, 2021), https://www.csoonline.com/article/570537/the-solarwinds-hack-timeline-who-knew-what-and-when.html.

[64] *Litigation Releases: SolarWinds Corp. and Timothy G. Brown*, SEC (Nov. 20, 2025), https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26423.

[65] "In June 2018, SolarWinds Network Engineer D identified a 'security gap' relating to SolarWinds' remote access virtual private network, which allowed access from devices not managed by SolarWinds. Network Engineer D warned that this setup

ongoing security shortfalls[66] were not acted upon,[67] potentially to minimize impact on corporate share price.[68] Indeed, the compromise of this key government safety tool apparently came to the attention of the public because of the efforts of external parties.[69] Additionally, according to the SEC complaint, company employees appear to have knowingly provided incorrect information to third parties in the aftermath.[70] Because of the safety design choices, *i.e.*, the alleged failure to maintain a

was 'not very secure' and later explained that someone exploiting the vulnerability 'can basically do whatever without us detecting it until it's too late' which could lead to a 'major reputation and financial loss' for SolarWinds." Complaint at 5, SEC v. SolarWinds Corp., No. 23-cv-9518 (S.D.N.Y. Oct. 30, 2023). "In November 2020, a SolarWinds information security employee sent an instant message to Senior Infosec Manager E with a link to a list of vulnerabilities in the Orion platform stating, 'The products are riddled and obviously have been for many years.' That same month, a SolarWinds network engineer complained, 'We filed more vulnerabilities then [sic] we fixed. And by fixed, it often means just a temporary fix… but the problem is still there and it's huge. I have no idea what we can do about it. Even if we start to hire like crazy, which we will most likely not, it will still take years. Can't really figure out how to unf**k this situation. Not good.'" *Id.* at 6.

[66] According to the SEC complaint, SolarWinds management failed to remedy known access control problems "for years." *Id.* at 3.

[67] "In and around the same time that SolarWinds was making . . . materially misleading public statements [about its security] . . . [i]nternal emails, messages, and documents describe numerous known material cybersecurity risks, control issues, and vulnerabilities. These internal statements dramatically contradict SolarWinds' public disclosures relating to its cyber security practices, risks, controls, and vulnerabilities." *Id.* at 4. For example, internal SolarWinds documents showed that "[i]n October 2018 . . . [SolarWinds CISO] Brown wrote in an internal presentation that SolarWinds' 'current state of security leaves us in a very vulnerable state for our critical assets.'" Id. at 2. Then, "[a]n August 2019 presentation warned that '[a]ccess and privilege to critical systems / data is inappropriate'" and "a July 2020 presentation . . . warned about threat actors' familiarity with a critical SolarWinds software platform, noting that the threat actors '[k]now how to deploy software, shut off backups, etc.'" *Id.* at 5.

[68] Warrell & Murphy, *supra* note 59. ("Shares in SolarWinds fell 15 per cent in early trading on Monday after news of the hack emerged."). According to the SEC complaint, Orion accounted for 45% of SolarWinds' revenue in 2020 and was its "crown jewel" asset. Complaint, *supra* note 65, at 2. "The stock price continued to drop and lost approximately 35% of its value by the end of the month as SolarWinds disclosed more details of the SUNBURST attack, and as news outlets reported that internal sources had warned SolarWinds for several years about the Company's cybersecurity risks and vulnerabilities." *Id.* at 9.

[69] Zetter, *supra* note 61.

[70] According to the SEC complaint, "[s]hortly after the October 2020 attack against Cybersecurity Firm B, SolarWinds employees including Brown recognized similarities between that attack and the attack on U.S. Government Agency A. But when personnel at Cybersecurity Firm B asked SolarWinds employees if they had previously seen similar activity, InfoSec Employee F falsely told Cybersecurity Firm B that they had not. He then messaged a colleague, '[W]ell I just lied.'" Complaint, *supra* note 65, at 8.

secure development lifecycle and the high degree of administrator access granted to certain corporate insider accounts,[71] the impact of the compromise was potentially amplified. Similarly, because of the nature of visibility into customer systems, the software seemed to offer a type of single point of failure with possible outsized impact in some cases,[72] raising the question of the robustness and adequacy of both SolarWinds' and customers' threat modeling to respond to the changing threat landscape.[73] If the media reports are to be believed, and "attackers . . . had 14 or more months of unfettered access," then it seems threat detection and incident response by SolarWinds and its customers were not optimal in practice. Ultimately, the SEC shifted its priorities and dismissed the enforcement action.[74] This dismissal illustrates that even

[71] *See id.* at 3, 27; *see also Advanced Persistent Threat Compromise*, *supra* note 59 ("CISA incident response investigations have identified that initial access in some cases was obtained by password guessing, password spraying, and inappropriately secured administrative credentials accessible via external remote access services.").

[72] Attackers gained access to network traffic management systems. *See Emergency Directives: ED 21-01: Mitigate SolarWinds Orion Code Compromise*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Dec. 13, 2020), https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise. For a complete discussion of deployment and lateral movement by threat actors in connection with the Solar Winds and related attacks, *see, e.g.*, *Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (last revised May 21, 2021), https://www.cisa.gov/news-events/analysis-reports/ar21-134a; Russian SVR Activities Related to SolarWinds Compromise, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (May 2021), https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Russian_SVR_Activities_Related_to_SolarWinds_Compromise_508C.pdf; *Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (May 14, 2021), https://www.cisa.gov/news-events/news/remediating-networks-affected-solarwinds-and-active-directorym365-compromise.

[73] SEC v. SolarWinds Corp., 741 F. Supp. 3d 37, 56, 81 (S.D.N.Y. 2024). While the U.S. District Court for the Southern District of New York sustained the SEC's claims of securities fraud based on the company's public Security Statement, it dismissed claims of securities fraud and false filings based on other statements and filings. *Id.* at 49–50. It also dismissed as "ill-pled the SEC's claims relating to SolarWinds' internal accounting and disclosure controls and procedures." *Id.* As a conceptual matter, it is likely that (different pleadings and) other courts may not arrive at the same outcome on this final point. As legal scholars have argued for decades, a public company's officers cannot reasonably attest to the integrity of the information in accounting and other financial internal control systems as required by Sarbanes-Oxley Section 404 if they have actual knowledge that they cannot also attest to the information security integrity of those systems as a technical matter. Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3.1 BERKELEY BUS. L.J. 129, 186 (2005).

[74] Joint Stipulation to Dismiss and Releases, SEC v. SolarWinds Corp., 1:23-cv-09518-PAE, (S.D.N.Y. Nov. 10, 2025) (Dkt. No. 202).

partial redress after a compromise may not be a given; securing strong warranties and audit rights through the procurement process is the first and best line of defense in avoiding irreparable harms.

Compromises such as the supply chain compromise above demonstrate the critical nature of obtaining audit rights, warranties of ongoing monitoring and patching, warranties of responsiveness to external third party reports, warranties of successful internal vulnerability handling processes, contractually-mandated immediate notification obligations in connection with known vulnerabilities, and other basic aspects of computer security governance that should play a key role in all technology procurement processes. Further, as Professor Elizabeth Rowe has argued, the procurement contracting process is similarly the correct place to address trade secrecy concerns, while preserving accountability.[75] Similarly, the level of security gaps highlighted in situations such as the supply chain compromise above illustrate the importance of continued robust agency enforcement, including actions under the False Claims Act[76] in connection with material computer security misrepresentations or failures to fulfil contractual warranties made as part of the procurement process.[77]

[75] "While recognizing that the owner of a trade secret who establishes that the requested information is in fact a trade secret may refuse to disclose it, the court found that this privilege is not absolute . . . . Apprehension about algorithmic transparency has increased further after *Food Marketing Institute v. Argus Leader Media*, in which the Supreme Court held that information is exempt from FOIA so long as the information is treated as confidential and its owner has received assurance that the information will remain confidential…·Another practical limitation of obtaining records through FOIA is that the government cannot give that which it does not possess. Therefore, to the extent private vendors retain ownership, control, and possession of their algorithmic models, records, and source codes, they remain beyond the reach of public records requests. There are also FOIA exemptions that protect law-enforcement and court records Thus, even outside the FOIA context, criminal defendants have been unsuccessful in obtaining algorithmic models and other proprietary information during discovery because it was in possession of the developer (not the government) and claimed as a trade secret." Rowe, *Procuring Algorithmic Transparency*, supra note 27, at 331, 335; Elizabeth A. Rowe & Harrison E. Kearby, *Trade Secrecy & the Government's Right to Repair*, 29 VA. J.L. & TECH. 7 (2026).

[76] False Claims Act, 31 U.S.C. §§ 3729–33.

[77] *See, e.g.*, *Raytheon Companies and Nightwing Group to Pay $8.4M to Resolve False Claims Act Allegations Relating to Non-Compliance with Cybersecurity Requirements in Federal Contracts*, DOJ (May 1, 2025), https://www.justice.gov/opa/pr/raytheon-companies-and-nightwing-group-pay-84m-resolve-false-claims-act-allegations-relating.

2. Integrity

In computer security, questions of integrity involve "guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity."[78] Consider the problem of robocalls, a technology integrity problem impacting both the private and public sectors, where callers misrepresent their identity, tricking consumers into answering their phones in order to listen to a recorded message or to be funneled by an automated system into a call center.[79] The problem of robocalls resulted in tens of thousands of consumer complaints to both the Federal Trade Commission and the Federal Communications Commission annually in the 2010s, yet the private sector solutions on the market were few, and those that existed were suboptimally effective. In response to this private sector supply side failure, the Federal Trade Commission (FTC) used two types of procurement authority in tandem that partially mitigated the consumer protection problem. For a limited time, the FTC maintained a funded role for a law professor to serve as an academic in residence and senior policy advisor,[80] which could be considered a procurement of human capital. In 2014, the FTC academic in residence collaborated with a group of attorneys and paralegals in the Bureau of Consumer Protection at the FTC to leverage a novel type of procurement authority — the authority to run procurement contests under the America Competes Act.[81]

[78] Jennifer Cawthra et al., *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*, NIST Spec. Publ'n No. 1800-26A, 1 (2020), https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html.

[79] *See Robocalls*, FTC CONSUMER ADVICE, https://consumer.ftc.gov/articles/robocalls (last accessed Jan. 30, 2026).

[80] *FTC Names Latanya Sweeney as Chief Technologist; Andrea Matwyshyn as Policy Advisor*, FTC (Nov. 18, 2013), https://www.ftc.gov/news-events/news/press-releases/2013/11/ftc-names-latanya-sweeney-chief-technologist-andrea-matwyshyn-policy-advisor.

[81] Kashmir Hil, *The FTC's Controversial Battle To Force Companies To Protect Your Data*, FORBES (Aug. 21, 2014), https://www.forbes.com/sites/kashmirhill/2014/08/21/the-ftcs-controversial-battle-to-force-companies-to-protect-your-data/. *See also* Camilla A. Hrdy, *Cluster Competition*, 20 LEWIS & CLARK L. REV. 981, 983 (2016) ("The most prominent example of the expanded federal role in cluster policy is the America COMPETES Act, which established a 'regional innovation program [(RIP)] to encourage and support the development of regional innovation strategies, including regional innovation clusters . . . .'"); Stuart Minor Benjamin & Arti K. Rai, *Fixing Innovation Policy: A Structural Perspective*, 77 GEO. WASH. L. REV. 1, 5 (2008) ("The America COMPETES Act passed in August 2007, provides, inter alia, for a 'President's Council on Innovation and Competitiveness' that will make recommendations on innovation policy. The Act envisions a Council with hortatory authority that would be composed of the heads of the major agencies whose actions affect innovation.");

Together, these two uses of procurement enabled the FTC to run a public contest and to stimulate the creation of new private sector solutions to robocalling.[82] Using the venue of the DEF CON security conference, the FTC ran a contest in the days leading up to the conference and on site where teams competed for prize money to develop the most effective technology. The winning team went on to form a fledgling company with the new technology, which was protectable as a matter of intellectual property, and in which the FTC chose to retain no interest. The FTC also created a snazzy t-shirt design to defend against impersonation of FTC staff at DEF CON, later releasing the design to the public as vector art through the internet, retaining no copyright interest.[83] In this way, the FTC used two atypical procurement authorities to push innovation in the private sector, addressing a public policy problem identified by consumer complaints.

Issues of integrity can also lead to unexpected out-of-band problems in procurement, such as a situation where the U.S. National Archives and Record Administration (NARA) faced a crisis due to a system with a hardware integrity shortcoming. After a server unexpectedly failed, sourcing a replacement became a challenge.[84] Like the FTC and DARPA, NARA used procurement through public contest. However, the results

Christopher S. Elmendorf & Darien Shanske, *Solving "Problems No One Has Solved": Courts, Causal Inference, and the Right to Education*, 2018 U. ILL. L. REV. 693, 718 (2018) ("[T]hrough the America Competes Act of 2007 . . . Congress required states to improve their educational data systems as a condition for receiving fiscal stabilization funds under the American Recovery and Reinvestment Act of 2009."); Greg Dotson, *Congress's Fifty Year Mission to Transition Motor Vehicles: A Brief History of Federal Electric Vehicle Policy in the United States*, 33 N.Y.U. ENV'T L.J. 93, 143 (2025) ("In 2007, Congress passed, and President Bush signed into law, the America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science Act (America COMPETES Act). This legislation boosted research on electric vehicles by establishing the Advanced Research Projects Agency – Energy (ARPA-E) in order to 'overcome the long-term and high-risk technological barriers in the development of energy technologies.'"); *Cyber!*, *supra* note 26, at 1193–94 ("[T]he FTC and the Defense Advanced Research Projects Agency (DARPA) have used contests under the America Competes Act, as renewed, as a way to stimulate entrepreneurship in security solutions. This type of contest approach should be expanded and used by other agencies to stimulate security entrepreneurship and creation of new security tools for both the public and private sector.").

[82] The contest was named Zapping Rachel, deriving the name from a fictional evil robocalling villain. *Zapping Rachel*, FTC, https://www.ftc.gov/news-events/contests/zapping-rachel (last accessed Jan. 30, 2026).

[83] *Id.* The t-shirts were purchased by the FTC employees who participated in the contest at their own expense (based on personal experience (and expense) of the author).

[84] *See* discussion *infra* Section I.B.3.

demonstrate the importance of careful procurement: the resulting contest winner included a potential counterfeit part.[85] This integrity problem highlights the need for including robust warranties regarding supply chain integrity and third-party verification into procurement processes. But the NARA server failure also offers an example of the third kind of computer security procurement dynamic, problems of availability.

3. Availability

Availability in computer security refers to "ensuring timely and reliable access to and use of information" on an as-needed basis.[86] When NARA's server failed and the replacement server from the contest included a potential counterfeit part, an availability problem arose at NARA: NARA employees were unable to access e-mail and the Internet for several days.[87]

But a second availability problem arose, one involving procurement. As explained by procurement expert Katherine John, NARA was unable to procure a replacement server through the U.S. General Services Administration's (GSA) Multiple Award Schedules due to required compliance with the Trade Agreements Act, which was also the reason that NARA used the contest procurement vehicle and held its own competition. [88] In addition to a potentially counterfeit part, the resulting server was not compatible with the NARA system, leading NARA to terminate the procurement and return the equipment.[89] As this case study signals, our conceptual model needs updating from a linear, unidirectional model to a model driven by nonlinear, bidirectional processes, the kind of processes that have led the United States to "progress" in past eras. Progress in procurement means fulfilling the goals of the process as set forth in the CFR and relevant statutes, while maintaining technological suitability for context; the point is appropriate technology, not necessarily newer technology.

But a second availability challenge in procurement arises in connection with security and the use of open source software products,

[85] Katherine M. John, *Information Technology Procurement in the United States and Canada: Reflecting on the Past with an Eye Towards the Future*, 48 PROCUREMENT L. 4, 6 (2013).

[86] Cawthra, *supra* note 78, at 1.

[87] John, *supra* note 85 at 6.

[88] *Id.*

[89] NARA finally procured the server it had originally wanted through a sole-source procurement. *Id.*

which are used widely in both the public[90] and private sector.[91] Many open source projects are provided without cost under open source licenses to the public; therefore, upfront procurement costs are shifted into nontraditional forms. While security testing and vetting of software tools and code libraries is a necessary procurement consideration for both proprietary products and open source alternatives, open source procurement can present a somewhat novel problem that comes up in a time sensitive manner in the context of computer security: a problem that might be called the "hit by a truck" problem. Many open-source projects are maintained by crowdsourced efforts of hobbyists or by a small number of dedicated contributors.[92] Thus, if one of them goes on vacation, chooses to stop contributing or, sadly, gets sick or hit by a truck, there may be no one capable of correcting the code and releasing a patch in a timely manner. Or consider the possibility of the lead contributor going on an extended leave; a coordination gap may exist and a patch is delayed, exposing both the public and private sector to the risk of exploitation by adversaries.[93] Imagine the scenario where the Heartbleed vulnerability, an infamous vulnerability in an open source code library that was widely in use in both the public and private sector,[94] had been maintained by only one person who happened to be on a remote hiking trip when the vulnerability was discovered. This "hit by a truck" problem remains unresolved in modern procurement. Another related critically important coordination problem that remains unresolved involves severe backlogs and government personnel shortages in vulnerability management, in addition to various data quality control problems that have plagued both private and public sector efforts

[90] For a discussion of public procurement and open-source software, see Jyh-An Lee, *New Perspectives on Public Goods Production: Policy Implications of Open Source Software*, 9 VAND. J. ENT. & TECH. L. 45, 62–64 (2006).

[91] *See generally* MARCO GEROSA & ADRIENN LAWSON, THE STATE OF GLOBAL OPEN SOURCE 2025 (The Linux Foundation, 2025).

[92] *Cf. Open Source Projects Looking for Contributors: A Starter Guide*, OSSSOFTWARE.ORG (Dec. 18, 2023) https://osssoftware.org/blog/open-source-projects-looking-for-contributors-a-starter-guide/; *Finding Ways to Contribute to Open Source on GitHub*, GITHUB DOCS, https://docs.github.com/en/get-started/exploring-projects-on-github/finding-ways-to-contribute-to-open-source-on-github (last visited Mar. 6, 2026).

[93] Josh Fruhlinger, *The Heartbleed Bug: How a Flaw in OpenSSL Caused a Security Crisis*, CSO (Sept. 6, 2022), https://www.csoonline.com/article/562859/the-heartbleed-bug-how-a-flaw-in-openssl-caused-a-security-crisis.html.

[94] Aurelija Einorytė, *What is Heartbleed? The Heartbleed Vulnerability Explained*, NORDVPN (Jan. 27, 2024), https://nordvpn.com/blog/what-is-heartbleed-bug/; Heartbleed Bug, OWASP.ORG (last accessed Jan. 30, 2025), https://owasp.org/www-community/vulnerabilities/Heartbleed_Bug.

on point for decades.[95] Private sector efforts have proven unable to address these security coordination challenges, setting up the stage for possible novel procurement strategies.

But a third challenge arises from a misalignment in perception that is bolstered by traditional models of procurement — that the private sector's interests are aligned with those of the broader public and the national interest. In some cases, they are not. In fact, in some cases they may be hostile to them. Consider the procurement nightmare that a California fire department faced in 2018. As wildfires raged and as Californians evacuated, the heroic efforts of firefighters to contain the blaze and issue safety communications were hindered by an unexpected foe: unavailability of Internet access. According to the firefighters, the ISP in question informed them in the middle of the public safety emergency that their Internet access had been throttled because the department had purchased an "incorrect" tier of service, and the firefighters perceived the representative to be more concerned with attempting to upsell the department on a higher tier of service than assisting them during the crisis.[96] Thus, procurement of consumer facing technology products and services can bring with it a set of hidden costs, and any next generation technology procurement model must adequately model future adversarial scenarios, like private sector profit motives sabotaging government procurement efforts.

But again, the future of technology procurement and any conceptual models that we use to embody it should recognize that these various procurement scenarios are not the traditional "pull" or agency version where government purchased goods and services are already available or easily produced in the private sector. The story of the government role in exponential technology improvements has historically been dramatically underestimated in modern retellings of technology history.[97]

Indeed, history offers numerous examples demonstrating that sometimes more creative procurement solutions are warranted to further technology progress. Three case studies in particular illustrate that both public and private sector benefits accrue where thoughtful and creative procurement solutions arise. Three such examples can be found in (1) the "archiving" of Mount Vernon as a historical site and the "backup"

[95] For a discussion of the challenges of security advisory writing, see *Who Reads Mega-advisories? No one! (Almost)*, JERICHO BLOG (Apr. 10, 2025), https://jericho.blog/2025/04/10/who-reads-mega-advisories-no-one-almost/ [https://perma.cc/S38R-AZDH].

[96] Andrea M. Matwyshyn, *Unavailable*, 81 U. PITT. L. REV. 349, 369 (2019).

[97] *See, e.g.*, MARIANA MAZZUCATO, THE ENTREPRENEURIAL STATE: DEBUNKING PUBLIC VS. PRIVATE SECTOR MYTHS 5 (2015).

of its records and information and the role of the National Archives and National Park Service, (2) the history of package delivery and its relationship to the U.S. Postal Service (USPS) and the evolution of internet commerce, and (3) the process of rural electrification and the role of the Rural Electrification Administration.

Consider the story of Mount Vernon and its historical preservation, or what might be reframed as a procurement story about the threats to availability of historical information from deterioration and deprecation. The archiving and "backup" of the physical structures and documentation of Mount Vernon and George Washington's life there offers an illustrative story of the challenges of accomplishing projects where no private sector provider is interested due to lack of profitability in the short term.[98] After his death, George Washington's estate was maintained by members of his family as long as feasible, but the estate fell into disrepair.[99] Washington's descendants sought to transfer possession and maintenance of Mount Vernon to the United States government or to the Commonwealth of Virginia, preserving its singular historical role in the Founding Era.[100] Unfortunately, Congress was unwilling to appropriate funding for this purpose at the time. Similarly, no private sector buyers were interested in purchasing the estate in order to preserve it as a national historical landmark.[101] Thus, the estate fell into tragic disrepair.[102] However, thanks to the efforts of Ann Pamela Cunningham and a small group of intrepid women who were horrified by the obvious irreparable harm to the public underway, our country's first national historic preservation society, the Mount Vernon Ladies' Association, sprang to life, purchased the estate, and crowdfunded

[98] Jeremy Musson, *Mount Vernon: The Story of George Washington's Country Estate*, COUNTRY LIFE (Oct. 6, 2024), https://www.countrylife.co.uk/architecture/mount-vernon-the-story-of-george-washingtons-country-estate-274150.

[99] Kate Egner & Zoie Horecny, *Ann Pamela Cunningham*, MOUNT VERNON (Mar. 11, 2025) ("What she saw inspired her to write her daughter, 'I was painfully distressed at the ruin and desolation of the home of Washington and the thought passed through my mind: Why was it that the women of his country did not try to keep it in repair, if the men could not do it? It does seem such a blot on our country!' . . . Cunningham was inspired by her mother's sentiments and took up the cause of purchasing and restoring Mount Vernon."), https://www.mountvernon.org/library/digitalhistory/digital-encyclopedia/article/ann-pamela-cunningham.

[100] *Id.* ("[John Augustine] Washington was initially unwilling to sell the estate unless Virginia or the United States was interested . . . .").

[101] *Id.*

[102] *Id.* (quoting Ann's mother writing in a letter that she was "painfully distressed at the ruin and desolation of the home of Washington" as she sailed past).

restoration.[103] Eventually, the procurement and appropriations error was corrected in part by a later Congress, and Mount Vernon and the Washington Presidential Library exist in a restored state today, staffed in part by federal employees[104] and protected by the watchful eye of a new generation of members of the Mount Vernon Ladies' Association.[105] The failure to preserve Washington's estate and his papers would have caused irreparable harm to the country.[106] Yet, much like the computer security challenges we face today,[107] convincing both private and public sector interests to take action in time-sensitive situations (in ways that seem obvious in hindsight) can prove difficult in the moment as an operational matter. As this story of (spectacular shortsightedness in) procurement demonstrates, private sector interests often do not align with the interests of the United States and its people, and the procurement process for major projects may sometimes involve decades of work and non-traditional collaborations between the public and government agencies.

A second case of historical unavailability problems that were solved through procurement involves the story of rural universal package delivery and the U.S. Postal Service. As explained by legal scholars, the ability to send packages through the U.S. mail arose as a response to a private sector availability failure: private sector package delivery companies were often intentionally excluding rural delivery addresses because they deemed delivery inadequately profitable.[108] In some parts of the country, service was simply unavailable or, when delivery of

[103] *The Mount Vernon Ladies' Association*, MOUNT VERNON, https://www.mountvernon.org/preservation/mount-vernon-ladies-association (last visited Mar. 6, 2026).

[104] *George Washington's Mount Vernon and Estates*, NAT'L PARK SERV., https://www.nps.gov/thingstodo/washingtons-mount-vernon-estates.htm (last visited Mar. 6, 2026); *George Washington Papers*, LIBR. CONGRESS, https://findingaids.loc.gov/repositories/19/resources/3115 (last visited Mar. 6, 2026).

[105]; *The Mount Vernon Ladies' Association*, *supra* note 103.

[106] Once a unique historical landmark is lost, recreation of its original form often presents challenges. For example, the recreation of the President's House of George Washington and John Adams in Philadelphia presented challenges in reconstruction after demolition and merely a symbolic shell exists on the spot today. *President's House Site*, NAT. PARK SERV., https://www.nps.gov/places/000/presidents-house-site.htm [https://perma.cc/Z53E-7PH6] (last visited Mar. 6, 2026).

[107] Andrea M. Matwyshyn, *It's Morning Again in Pennsylvania: Rebooting Computer Security Through a Bureau of Technology Safety*, LAWFARE (Jan. 30, 2024), https://www.lawfaremedia.org/article/it-s-morning-again-in-pennsylvania-rebooting-computer-security-through-a-bureau-of-technology-safety.

[108] Matwyshyn, *Unavailable*, *supra* note 96, at 382 (explaining that when the first post office was opening in 1775 in Philadelphia it was chartered to only deliver newsletters and personal correspondence, leaving parcel delivery to the private sector by choice).

packages to rural addresses occurred, the shipping costs were often financially prohibitive for the public.[109] As a consequence, the (intentionally circumscribed)[110] mandate of the Post Office was expanded in 1916 to address the market failure in package delivery to meet the needs of the public (and additional staff and facilities were acquired) — an illustration of the divergent goals of public services and private sector interests.[111] Yet, the resolution of the rural package delivery failure not only fixed the quality of services for millions of consumers, it also caused an explosion of other private sector technology progress. The mail order catalog industry suddenly began to flourish because the key stumbling block to its success had been resolved. Later, the mail order catalog model would become the conceptual model for the e-commerce explosion of the 1990s, another commercial boon that arose primarily because of government procurement and the creation of the internet.[112] Today, USPS parcel delivery also plays a critical role as infrastructure core to national security countermeasures in case of a biological attack.[113]

A third story of technology availability challenges solved through creative procurement involves the history of rural electrification. Much like the history of rural parcel delivery, the history of rural electrification offers an example of a situation where market profitability incentives were inadequate to engage the private sector's interest in solving a social problem. Although large cities such as New York City were mostly electrified as early as the late 1800s,[114] rural communities were largely unable to participate in the emerging technology economy powered by electrification at the time.[115] Indeed, rural electrification in the United States only reached approximately 3.2% of farming households in 1925.[116] Consequently, rural electrification was one of the priorities of

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *Id.* at 383.

[113] *Id.*

[114] N.Y.C. Dep't of Records & Info. Servs., *Electrification Educational Aid* (2020), https://www.nyc.gov/assets/records/pdf/Education/Electrification%20Educational%20Aid.pdf.

[115] Harold D. Wallace, Jr., *Power from the People: Rural Electrification Brought More Than Lights*, NAT'L MUSEUM AM. HIST. (Feb. 12, 2016), https://americanhistory.si.edu/explore/stories/power-people-rural-electrification-brought-more-lights [https://perma.cc/KAN7-SEQC].

[116] Maddie Fowler, *Refrigerators and Women's Empowerment: The "Peaceful Revolution" of Rural Electrification*, NAT'L MUSEUM AM. HIST. (Oct. 20, 2021), https://americanhistory.si.edu/explore/stories/refrigerators-and-womens-

post-WWI recovery and domestic resiliency efforts, and through Congressional action and appropriation for procurement, the Rural Electrification Administration was established in 1936.[117] In particular, creative appropriation and procurement allowed for solving two problems: infrastructure buildout and public education. Private utility companies were unwilling to provide universal service, offering incomplete proposals that exceeded budgeted amounts for the project of farm electrification.[118] A more cost-effective solution arose through the REA taking the lead itself in a light-touch, decentralized approach: REA launched a novel loan program that provided startup capital to farming communities to build their own electricity infrastructure with loans repayable over a 30 year term. But, perhaps even more importantly, REA hired key personnel to establish what would come to be known as the "Electric Circus," a traveling small team of electricity specialists.[119] Led by Louisan Mamer,[120] the Electric Circus team crisscrossed the country, teaching the public about the benefits and safety concerns of electricity, and assisting local communities in using the loan program to establish their own locally owned, managed, and operated rural electricity cooperatives.[121] Through the efforts of the REA and the Electric Circus team, by 1950, 90% of farms were electrified.[122] In other words, the technical problem of electrical infrastructure for farms was more cost-effectively addressed through a small group of humans and bottom-up solutions, rather than through a large scale top-down private sector procurement process. In this way, a new government agency using a restrained government procurement approach centered around humans was able to stimulate dramatic technology progress. It corrected availability deficits when the private sector would not. It is precisely this

empowerment-peaceful-revolution-rural-electrification [https://perma.cc/9CM9-HU58].

[117] Tim Sablik, *Electrifying Rural America*, FED. RSRV. BANK OF RICHMOND, ECON FOCUS Q1 (2020), https://www.richmondfed.org/publications/research/econ_focus/2020/q1/economic_history.

[118] *Id.*

[119] Fowler, *supra* note 116.

[120] Wallace, *supra* note 115. As explained by Mamer's archives at the Smithsonian Institution, "[l]ight plays a large part in producing food and fiber . . . . Indirectly, good light contributes to increased production . . . . In saving time, light ranks second only to running water among farm and home electrical uses . . . . Good lighting depends on adequate wiring system, proper selection of lamps and fixtures, . . . and proper care and replacement of lamp bulbs or tubes." *Louisan E. Mamer Rural Electrification Administration Papers*, NAT. MUSEUM AM. HIST., https://edan.si.edu/slideshow/viewer/?eadrefid=NMAH.AC.0862_ref30.

[121] Wallace, *supra* note 115.

[122] Fowler, *supra* note 116.

collaborative model, one between expert humans and tailored technological approaches, that reflects the most promising model for both the future of technology procurement and our technology economy: a model of human-machine symbiosis.

C. Human-Machine Symbiosis

As both public and private sector systems begin to incorporate various forms of (technologies known colloquially as)[123] AI, procurement processes and plans around acquisition and management of said AI often fail to recognize two important shifts that are already manifesting in computer security contexts. The first shift involves the changed nature and pace of human-computer interactions in a computer environment moving toward a state of what is known in computing industry circles as "human-machine symbiosis." The second shift is in the changed nature of corresponding threat models presented by human-machine symbiosis.

The concept of human-machine symbiosis is attributed to a seminal paper by psychologist and head of the Information Processing Techniques Office at ARPA J.C.R. Licklider[124] in 1960 called *Man-Computer Symbiosis*. In the piece, Licklider explains a model of human-machine cooperation that sits "[b]etween 'Mechanically Extended Man' and 'Artificial Intelligence.'" Licklider elaborates:

> In the man-machine systems of the past, the human operator supplied the initiative, the direction, the integration, and the criterion. The mechanical parts of the systems were mere extensions, first of the human arm, then of the human eye. These systems certainly did not consist of "dissimilar organisms living together . . ." There was only one kind of organism-man-and the rest was there only to help him . . . [but] a fantastic change has taken place during the last few years. "Mechanical extension" has given way to replacement of men, to automation . . . the human operators are responsible mainly for functions that it proved infeasible to automate. Such systems . . . are "semi-automatic"

[123] J.C.R. Licklider, *Man-Computer Symbiosis*, IRE TRANSACTIONS ON HUMAN FACTORS ELECS. 4, 4–11 (1960) https://groups.csail.mit.edu/medg/people/psz/Licklider.html.

[124] Licklider's leadership is credited with launching and funding ARPANET, the precursor to today's internet. *J.C.R. Licklider*, INTERNET HALL OF FAME https://www.internethalloffame.org/inductee/jcr-licklider/.

> systems, systems that started out to be fully automatic but fell short of the goal.[125]

In other words, Licklider highlights the trend that he was already noting in 1960 of the substitution of some kinds of human labor with the automation of machine processing. He similarly highlights that these attempts at automation regularly did not succeed at full automation, still requiring humans to work with them for key parts of their functionality. The machines and the humans each added different skills to the shared process.

Licklider further explains:

> [A] main aim is . . . to bring computing machines effectively into processes of thinking that must go on in "real time," time that moves too fast to permit using computers in conventional ways. Imagine trying, for example, to direct a battle with the aid of a computer on such a schedule as this. You formulate your problem today. Tomorrow you spend with a programmer. Next week the computer devotes 5 minutes to assembling your program and 47 seconds to calculating the answer to your problem. You get a sheet of paper 20 feet long, full of numbers that, instead of providing a final solution, only suggest a tactic that should be explored by simulation. Obviously, the battle would be over before the second step in its planning was begun. To think in interaction with a computer in the same way that you think with a colleague whose competence supplements your own will require much tighter coupling between man and machine than is suggested by the example and than is possible today.[126]

These separable, complementary modalities of real time thinking, in Licklider's view, offer the path forward to stimulate progress in both practical and conceptual ways.[127] He explains that this symbiosis between

[125] Licklider, *Man-Computer Symbiosis*, *supra* note 123, at 4.

[126] *Id.* at 5.

[127] *Id.* at 6–7 ("It seems likely that the contributions of human operators and equipment will blend together so completely in many operations that it will be difficult to separate them neatly in analysis. That would be the case it; in gathering data on which to base a decision, for example, both the man and the computer came up with relevant precedents from experience and if the computer then suggested a course of action that agreed with the man's intuitive judgment. [In theorem-proving programs, computers find precedents in experience, and in the SAGE System, they suggest courses of action. The foregoing is not a far-fetched example.] In other

humans and machines will create a set of circumstances where humans "will set the goals and supply the motivations, . . . formulate hypotheses, . . . ask questions, . . . think of mechanisms, procedures, and models, . . . [and] define criteria and serve as evaluators, judging the contributions of the equipment and guiding the general line of thought." They will also "handle the very-low-probability situations."[128]

For the last decade, this model of human-machine symbiosis has been tested in some computer security contexts. Again, the key role of procurement policy and its innovation-stimulating potential has been on display: one particularly successful example of a human-machine symbiosis experiment occurred at the DEF CON security conference in 2016. At the security conference, DARPA sponsored a so-called "CyberGrand Challenge" of the world's first all machine hacking tournament,[129] creating a sandboxed[130] field of battle for a tournament of "automatic defensive systems capable of reasoning about flaws, formulating patches and deploying them on a network in real time."[131] In this contest,[132] machine teams competed against each other for prize money and bragging rights.[133] The winning machine then competed in a challenge against human security experts and lost,[134] again potentially pointing to the benefits of a human-machine symbiotic model.[135]

operations, however, the contributions of men and equipment will be to some extent separable.").

[128] *Id.* at 7.

[129] DARPATV, *Darpa's Cyber Grand Challenge: Final Event Program*, at 1:00 (YouTube Aug. 8, 2016), https://www.youtube.com/watch?v=n0kn4mDXY6I.

[130] *Id.* at 14:50. For a discussion of sandboxing as a security technique, see Fortinet, *What is sandboxing?*, https://www.fortinet.com/resources/cyberglossary/what-is-sandboxing (last visited Mar. 6, 2026).

[131] *CGC: Cyber Grand Challenge*, DARPA (2016), https://www.darpa.mil/research/programs/cyber-grand-challenge.

[132] The contest was jocularly narrated by an astrophysicist and two computer security experts to a packed ballroom in the Paris hotel in Las Vegas. DARPATV, *supra* note 129, at 3:00.

[133] The winning team was an outgrowth of a lab at Carnegie Mellon University, outperforming private sector defense contractor teams. *See DARPA Celebrates Cyber Grand Challenge Winners*, DARPA (Aug. 5, 2016), https://www.darpa.mil/news/2016/cyber-grand-challenge-winners; Devin Coldewey, *Carnegie Mellon's Mayhem AI Takes Home $2 Million from DARPA's Cyber Grand Challenge*, TECHCRUNCH (Aug. 5, 2016), https://techcrunch.com/2016/08/05/carnegie-mellons-mayhem-ai-takes-home-2-million-from-darpas-cyber-grand-challenge.

[134] *2016 DEF CON CTF Final Scores*, LEGITIMATE BUS. SYNDICATE (2016), https://blog.legitbs.net/2016/09/2016-def-con-ctf-final-scores.html.

[135] Subsequent iterations of automated patching and defense systems continue to improve on their capabilities. *See, e.g.*, Matt Kapko, *DARPA AI Cyber Challenge Reveals Winning Models for Automated Vulnerability Discovery and Patching*, CYBERSCOOP

But still another element of human-machine symbiosis warrants consideration: the inevitability of needing to plan for the crisis management of machine-made disasters in real time, some of which may threaten to cause irreparable harms. As the long list of suboptimal outcomes at the introduction of this Essay implies, when viewed critically, today's (over)hyped technologies that purport to be able to fully replace humans in autonomous operations regularly fail in their self-assigned roles.[136] Worse, as scholars have explained at length elsewhere, all too often, modern technologies simply offer modern spins on fraud. **[137]** For example, some technology contractors push technology autonomy maximalism on government and consumers while simultaneously expressing concern over the potential of their own technologies to cause irreparable harms to society[138] — a self-contradiction that is difficult to reconcile. As such, caution is warranted in procurement, as is ensuring that procurement agreements memorialize requirements for various safety-enhancing measures regarding monitoring, archiving, correction, and audit.[139] As the history of both engineering[140] and technology disasters teaches us,[141] attempts at introducing innovation into sensitive contexts often fail spectacularly and interested parties regularly hide the extent of the disaster and its harms.[142]

As the next section explains, the problematic dynamics and irreparable harms described above push us to reconsider our models for technology procurement. It is time to recognize the changed relationship

(Aug. 8, 2025), https://cyberscoop.com/darpa-ai-cyber-challenge-winners-def-con-2025/ [https://perma.cc/JRP5-R33A].

[136] *See supra* Introduction.

[137] Matwyshyn, *Exploit Machina*, *supra* note 27.

[138] *Id.*

[139] For example, procurement requirements should consider logging of technical behaviors in detail to allow for reconstruction of conduct and decisions, to build systems with the capacity to "unlearn" errors arising from problematic training data, restore themselves to prior states, submit to human override, and allow for full technical security audit on a regular basis.

[140] Andrea M. Matwyshyn, *Keynote, Day 2: Homicideware*, BSIDELV (Aug. 7, 2024), https://www.youtube.com/watch?v=yCd-nQdzTcY; Andrea M. Matwyshyn, *Homicideware* (draft on file with author).

[141] Andrea M. Matwyshyn, *Corporate Cyborgs and Technology Risks*, 11 MINN. J.L. SCI. & TECH. 573, 574, 580, 583–84 (2010) (explaining the history of the Books and Records Crisis when automation was introduced into the New York Stock Exchange with disastrous results).

[142] The stakes are particularly high in computer security contexts. For a discussion of how modern computer security deficits are spiraling into predictably problematic disaster territory, see Andrea M. Matwyshyn, *It's Morning Again in Pennsylvania: Rebooting Computer Security Through a Bureau of Technology Safety*, LAWFARE (Jan. 30, 2024), https://www.lawfaremedia.org/article/it-s-morning-again-in-pennsylvania-rebooting-computer-security-through-a-bureau-of-technology-safety.

of procurement to the technology ecosystem; it is also time to refocus our procurement strategies around resilience and progress, not merely novelty and speed at the expense of safety.

II. THE NESTED MODEL OF TECHNOLOGY PROCUREMENT

Yet, in holding scientific research and discovery in respect, as we should, we must also be alert to the equal and opposite danger that public policy could itself become the captive of a scientific-technological elite.

– President Dwight D. Eisenhower[143]

As a thought exercise to shed light on the complex dynamics of technology procurement, let us briefly consider a very different "procurement" scenario. Imagine that you are sent as a trusted envoy by a table full of your friends to the bar, charged with procuring a pitcher of a highly carbonated beverage, such as beer or ginger soda. Prior to each "end user" pouring the beverage into a glass to consume, a series of invisible trusted steps has occurred. The ingredients that compose the beverage were grown, curated, processed, transformed, packaged, and conveyed in a complex supply chain that ended in a tap in a third-party owned establishment. The liquid was then deployed into a pitcher by either a machine or a human, whose skill is relevant in the quality of the end product. As anyone who has gone through the Guinness Academy Experience[144] knows, angling a glass or a pitcher improperly can result in disastrous foam consequences with a carbonated beverage, and skill in the art matters.[145] Assuming that deployment of the liquid into the pitcher has been successful, a particular proportion of immediately drinkable liquid and immediately non-drinkable foam exists in the pitcher. Then, secondary deployment occurs into individual glasses for the members of the public, who will consume the beverage. Once deployed into a glass, the beverage displays changing properties. Bubbles of carbonation travel up and down inside the glass with vigor. A foamy head progressively deteriorates as the beverage rests in the glass, with the ideal consumption conditions occurring sometime after the first pour, but before the foamy head deteriorates entirely. The flavor profile and

[143] *Eisenhower's Farewell Address*, *supra* note 1.

[144] *See Review of Guinness Storehouse*, TRIPADVISOR, https://www.tripadvisor.com/ShowUserReviews-g186605-d189694-r894399864-Guinness_Storehouse-Dublin_County_Dublin.html (last visited Feb. 5, 2026).

[145] *See Discussion of the "Most Common Beer Pouring Mistakes"*, BEERADVOCATE (Feb. 14, 2023), https://www.beeradvocate.com/community/threads/the-most-common-beer-pouring-mistakes.671439 (last visited Feb. 5, 2026).

utility of the liquid itself will also change overtime. If any point of the supply chain is compromised through contamination or failures of skill, the end product of a beverage in a glass may become unusable or even potentially physically injurious. The method of presentation, a glass pitcher and a glass pint, is also inherently fragile, though more resilient than, for example, a crystal brandy snifter. Understanding the properties and limitations of the liquid containment units are similarly critical to successful completion of the beverage mission of conveying consumable beverages to the end users. Further, a subsequent deployment of the beverage into a pitcher and into pint glasses may go horribly wrong, presenting a different experience because of changed conditions at any point in the supply chain of the product and service. As a consequence, the threat modeling and anticipation of how beverage deployment mishaps may alter the experience for the end user are also (beverage) mission critical. They will assist with success, as will audit, evolution of the process, and quality control improvements in situations where beverage disaster strikes.

Perhaps surprisingly, this metaphor of a pint of carbonated beverage offers us a loose mental model for some of the conceptual elements of a model for next generation technology procurement. Much like compromises of the integrity of a beverage, supply chain compromises can prove destructive to a technology product, its deployment, and the successful completion of a particular goal. Just as brewer hygiene is outcome determinative in the quality of a beverage,[146] so too security hygiene is outcome determinative in the quality of a technology product.[147] Just as a stale beverage in a glass deteriorates in quality over time, so too do technology products become stale due to unpatched security flaws and incompatibility with newer technologies. Just as a limited window exists for consuming a carbonated beverage before it goes flat, so too does a limited optimal window for use exist with particular technologies. Further, the context of the deployment of the technology and the skill of a team are critical elements in threat modeling and audit calculations. Just as one would offer ginger beer or nonalcoholic beer to a friend who does not consume alcoholic beverages, so too does selecting technologies for particular deployment contexts

[146] Sarah Buckholtz, *6 Ways to Maintain a Clean and Sanitized Brewery*, UNTAPPD (Sept. 12, 2022) ("[T]here's a common belief in the industry that brewing is ninety percent cleaning and ten percent actually brewing."), https://lounge.untappd.com/6-ways-to-maintain-a-clean-and-sanitized-brewery/.

[147] *Cyber Hygiene Services*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/cyber-hygiene-services (last visited Mar. 15, 2026).

require meaningful understanding of the end users and their self-defined needs.

Shifting from the beverage metaphor back to technology procurement directly, the next section builds on prior discussions of reciprocal security vulnerability and human-machine symbiosis to argue that resilience and progress should operate as shared animating values for future technology procurement. Building on these values, the section then offers a novel nested model that recognizes the changing dynamics of the technology procurement ecosystem, the Procurement in Nested Technology model or PINT.

A. Shared Baselines for a New Model

Two elements are critical in any successful model of technology procurement: resilience and progress.

1. Resilience

While the term resilience can have multiple meanings, [148] as defined by the National Institute of Standards and Technology in the context of security, resilience refers to "[t]he ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.[149] In the context of procurement,

[148] As explained by the Congressional Research Service:

> The term resilience can have multiple meanings and be applied to individuals and populations, networks and ecosystems, materials and structures, and other objects and human constructs. How someone understands resilience is often tied to the context in which it is applied, and the object of what is, or is to be, resilient (e.g., a person, a building). One definition for resilience asserts it's "the quality or fact of being able to recover quickly or easily from, or resist being affected by, a misfortune, shock, illness, etc." This largely figurative definition of resilience highlights the importance of clarifying the term's use within an organization or group, particularly where matters of policy and action are expected. . . .
>
> For example, concerning the topic of "Climate Change Adaptation and Resilience" (DOD Directive 4715.21), DOD has defined resilience as the "ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions."

Cong. Rsch. Serv., *Military Installation Resilience: What Does It Mean?* 1–2 (Jan. 6, 2021), https://apps.dtic.mil/sti/pdfs/AD1147490.pdf (last visited Feb. 5, 2026).

[149] Nat'l Inst. Standards & Tech., *Special Publication 800-39* app. at B-5 (Mar. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

the lessons of resilience analysis are twofold: first, resilience asks us to consider the impact of procurement choices on the ability to "bounce back" from the possibility of a total procurement failure and on the ability to mitigate failure as it is underway. As the procurement disasters at the beginning of this Essay illustrate, certain types of negative consequences in procurement decisions carry with them irreparable harms. Thus, procurement decisions, particularly those that directly or indirectly implicate irreparable harms, should by design include a "safety valve" for harmed individuals or groups, facilitating their ability to alert a procuring organization to harmful consequences. Then, these reports of harm should have clear pathways for analysis and trigger meaningful corrective responses in real time.[150] Second, resilience analysis encourages us to expressly consider security risk and formally threat model both threats and responses to various scenarios, seeking redundancy measures to bolster the speed of a "bounce back." A portion of this analysis includes leveraging procurement to advance technological collaboration, which bolsters resilience, both with the public and with other government agencies at the state and federal level. Indeed, the power of the procurement purse in pushing national resilience holds great promise.

2. Progress

The key role of government procurement in countries' technological advancement has been more expressly recognized by technology peer countries internationally.[151] For example, as described by the OECD, "Governments are increasingly recognising [sic][152] the immense power

[150] Particularly in light of current deficits in whistleblower channels for contractors, this consideration of safety valves for reporting as part of broader resilience adds value. For a discussion of suggested improvements to whistleblower protection, see *Whistleblowers: Key Practices for Congress to Consider When Receiving and Referring Information*, GEN. ACCT. OFF. (May 7, 2019), https://www.gao.gov/products/gao-19-432.

[151] "One of the policies that has received greater attention by both academics and practitioners, in recent years, is frequently termed 'public procurement for innovation.' This policy is often construed as a demand-side approach of a broader policy of promoting innovation in a particular industry In fact, several academics and practitioners tend to include public procurement policy within a subset of policies for innovation, and that tension for the primacy of policy foreshadows a larger issue of how to design these policies in ways that allow for harmonious coexistence." Fernando Mendoza Lopez & Joni Hersch, *Socioeconomic Policies in Public Procurement: What Should We Be Asking of Public Procurement Systems?*, 52 U. MEM. L. REV. 155, 183–84 (2021).

of public procurement to solve global societal challenges, improve productivity and boost innovation, while ensuring value for money. Public procurement represents 12% of gross domestic product (GDP) and 29% of total government expenditures on average across OECD countries, a clear sign of its potential to support broader policy objectives, including the fostering of innovation."[153] Domestically, as U.S. procurement scholars have noted, the role of procurement policy serving a broader function in the United States is "almost as old as the procurement function itself,"[154] even if not expressly acknowledged in law.

Our country's central source of shared baselines is the set of checks and balances set forth in the federalist structures created by our Constitution. The spending power of Article I, Section 8, Clause 1 presents one logical hook for the policies that underpin procurement, explaining Congress' power to "provide for the common defense and general Welfare" of the United States.[155] However, it also might be argued that a second Clause contains a related articulation of public policy values that impact procurement — the public policy value of promoting progress set forth in Article I, Section 8, Clause 8. Specifically in Clause 8, before granting Congress the power to secure periods of limited exclusivity for authors and inventors in their writings and discoveries, the Framers first memorialized the broader public policy

[153] OECD, PUBLIC PROCUREMENT FOR INNOVATION: GOOD PRACTICES AND STRATEGIES 3 (2017), http://dx.doi.org/10.1787/9789264265820-en.

[154] "The explicit use of public procurement to achieve broader societal goals is a practice almost as old as the procurement function itself. In the United States, early development of the federal procurement law was closely entwined with the military warranting a preference for domestic suppliers due to national security concerns. In fact, most governments around the world have identified the government's purchasing power as a tool to leverage the attainment of socioeconomic policy goals…Procurement officials are required to strive for efficient purchasing. Efficiency can be defined broadly to integrate the economic benefits from diverse objectives such as competition, integrity, customer satisfaction, and wealth distribution, among others." Mendoza & Hersch, *supra* note 169, at 157–58.

[155] U.S. CONST. art. I, § 8, cl.8.

goal: "[t]o promote the Progress of Science[156] and useful Arts."[157] During the last century, many of the most transformative new technologies that flourished in the private sector began their lives as appropriated projects.[158] In other words, the importance of government procurement dynamics in stimulating progress in science and useful arts is central; these are situations where the U.S. government did not merely "pull" from the private sector but instead "pushed" new technologies into it because of procurement. This push through procurement was the source of inventions whose derivative works were then subsequently developed in various forms by private sector entities (often into products that are themselves protectable under intellectual property law).[159]

But if we are to recognize these progress concerns as an animating element of a new procurement model, we should perhaps first ask what the Founders precisely meant in their choice of it for the first part of Clause 8. Indeed, a reading in this way creates a connection between the Congressional powers of Article I, Section 8, Clause 1, and the choice reflected in procurement contracting decisions of whether the U.S. government should obtain intellectual property rights to the goods and services created in the process of procurement. Yet no scholarship in the

[156] As articulated by the Supreme Court in *Golan v. Holder*, the "Progress of Science," at the time of the Framing, referred to "the creation and spread of knowledge and learning." 565 U.S. 302, 324 (2012) (citation omitted).

In modern philosophy, as explained by Professor Ilkka Niiniluoto:

> [Four] different types of progress can be distinguished relative to science: *economical* (the increased funding of scientific (research), *professional* (the rising status of the scientists and their academic institutions in the society), *educational* (the increased skill and expertise of the scientists), *methodical* (the invention of new methods of research, the refinement of scientific instruments), and *cognitive* (increase or advancement of scientific knowledge).

Ilkka Niiniluoto, *Scientific Progress*, STAN. ENCYC. PHIL. (Jan. 22, 2024), https://plato.stanford.edu/entries/scientific-progress (last visited Feb. 5, 2026).

[157] According to the Supreme Court in Graham v. John Deere Co. of Kansas City, "Progress of . . . . useful Arts" refers to encouragement of technological "innovation, advancement, or social benefit." *See* 383 U.S. 1, 6 (1966). However, textual sources from the Founding Era arguably do not support the Supreme Court's inclusion of the word "innovation." *See infra* text accompanying nn.175–76.

[158] The internet and global positioning systems are but two examples of government procurement, understood broadly, leading to transformational technological change. Wyskiel, *supra* note 43.

[159] Further, the remainder of the Clause and its focus on intellectual property connects with some of the challenges previously discussed with respect to technology procurement—various models of creation, dynamics of procurement process, and their relationship to intellectual property concerns. *See supra* Part I.

legal literature currently explores this Clause 1 and Clause 8 connection directly through the lens of "progress."

Legal scholars have afforded much consideration to understanding progress in Clause 8 in connection with intellectual property law, both as a matter of constitutional interpretation and as a matter of practice, [160] leading to interpretive debates among scholars.[161] In particular, Professor Dotan Oliar argues that based on the rejected language of draft clauses, we should understand that "the Progress [language] was added as a limitation."[162] As such, it can be argued that the promotion of progress holds meaning as a stand-alone policy articulation. [163]

How does technology fit into the policy instruction to Congress to "promote the Progress of Science and useful Arts"? The Supreme Court

[160] Jessica Silbey, *Promoting Progress: A Qualitative Analysis of Creative and Innovative Production*, in THE SAGE HANDBOOK OF INTELLECTUAL PROPERTY 515 (Matthew David & Debora Halbert eds., 2014) (explaining that "[n]otably, it is not a value-neutral or subjective concept but a tall order and one that interviewees describe as demanding objective evaluation. Progress is explicitly directional and qualitative: it is about novelty and correction vis-à-vis the past, and it is valued for the kinds of things produced and their associated benefits rather than for how much is made or money earned. Everyday work, professional identity and sustainable social welfare are signs of progress for almost all of the people and industry leaders I interviewed"), https://scholarship.law.bu.edu/faculty_scholarship/1377.

[161] Professor Malla Pollack argues that based on a review of five definitions of progress as used in the Pennsylvania Gazette and related information, progress was most commonly used to indicate some type of physical movement or spread. Malla Pollack, *What is Congress Supposed to Promote?: Defining "Progress" in Article I, Section 8, Clause 8 of the United States Constitution, or Introducing the Progress Clause*, 80 NEB. L. REV. 754 (2001). However, as explained by Professor Jake Linford, "the 'spread' definition has not been embraced by the majority of scholars. Instead, most scholars have embraced a series of meanings that coalesce around the notion that progress means advancement in knowledge . . . . Advancement can then be measured either in quantitative increase or qualitative improvement." Jake Linford, *Datamining the Meaning(s) of Progress*, 2017 BYU L. REV. 1531, 1545–46 (2017).

[162] Dotan Oliar, *Making Sense of the Intellectual Property Clause: Promotion of Progress as a Limitation on Congress's Intellectual Property Power*, 94 GEO. L.J. 1771, 1776 (2006) (arguing "the Framers intended the first part of the Clause — 'to promote the progress of science and useful art' — to be a limitation on Congress's intellectual property power"). In the specific context of copyright, some scholars understand this progress limitation to intentionally exclude fine art. *See, e.g.*, Barton Beebe, Bleistein, *The Problem of Aesthetic Progress, and the Making of American Copyright Law*, 117 COLUM. L. REV. 319, 338 (2017) (concluding from the drafting evidence that the decision of the Framers to exclude "fine arts from the language of the Progress Clause appears to have been a deliberate act").

[163] Similarly, it can be argued that national security concerns form a stand-alone priority apart from Article I, Section 8, Clause 1, supported by the fact that national security concerns appear again in later parts of the Constitution in a different form. *See, e.g.*, U.S. CONST. art. IV, § 4 ("The United States shall guarantee to every State in this Union a Republican Form of Government, and shall protect each of them against Invasion . . . .").

has offered only limited guidance. Modern Congressional annotations to the Constitution ascribe commentary in two Supreme Court cases in particular — *Golan v. Holder* and *Graham v. John Deere Co. of Kansas City.*[164] As explained in the Congressional annotations, the Progress language can be divided into two parts — progress of science and progress of useful arts; technology falls under the "useful arts."[165]

Turning to Constitutional history, Clause 8 caused very little controversy at the Constitutional Convention,[166] leaving us an impoverished historical record compared to other clauses in the Constitution. But, we have at least two sources of historical insight on the original meaning of "promote the Progress of Science and useful Arts" as it was likely understood by the Framers. The first involves standard dictionary definitions at the time. The second involves historians' and philosophers' analyses of the meaning of "progress" in the Founding and Framing Era.

Looking to period dictionaries, they tell us that "progress" refers to a forward trajectory.[167] It is noteworthy that these dictionaries also include the word "innovation," meaning novelty.[168] Thus, what we can deduce from the existence of both words at the time is that the Framers' choice away from the word innovation in favor of the word progress was intentional. In a consonant insight on the Framer's likely view of progress, Professor Jill Lepore explains that during the Founding Era, the term "innovation" had a negative connotation, and the Founders and Framers likely regarded innovation as an undesirable form of social

[164] *ArtI.S8.C8.1 Overview of Congress's Power Over Intellectual Property*, CONST. ANNOTATED, https://constitution.congress.gov/browse/essay/artI-S8-C8-1/ALDE_00013060/ (citing to *Golan* and *Graham* for the proposition that "The Progress of Science, at the time of the Framing, referred to the creation and spread of knowledge and learning").

[165] *Id.*

[166] Edward C. Walterscheid, *The Preambular Argument: The Dubious Premise of Eldred v. Ashcroft*, 44 IDEA J.L. & TECH. 331, 351 n.105 (2004) (citing 2 RECORDS OF THE FEDERAL CONVENTION 508–10 (Max Farrand ed., 1911)) (stating that James Madison's notes from the Constitutional Convention "indicate only that the Clause was approved without debate or dissent").

[167] *Progress*, 2 SAMUEL JOHNSON, A DICTIONARY OF THE ENGLISH LANGUAGE 404 (1766) [hereinafter *Progress*, JOHNSON] (stating the definition of progress as "[t]o move forward"), https://archive.org/details/dictionaryofengl02johnuoft/page/n403/mode/2up.

[168] *See, e.g.*, *Innovation*, 1 SAMUEL JOHNSON, A DICTIONARY OF THE ENGLISH LANGUAGE 1046 (6th ed. 1785) [hereinafter *Innovation*, JOHNSON], https://publicdomainreview.org/collection/samuel-johnson-s-dictionary-of-the-english-language-1785/ (stating the definition of innovation as "[c]hange by the introduction of novelty").

instability.[169] As a consequence, in choosing language for the Constitution, the Framers would not have chosen a word that would introduce (potentially socially destructive) novelty.[170] Instead, as reflected in Article I, Section 8, Clause 8, the Framers picked "Progress," a term that carried with it a normative component of improvement and advancement forward.[171] To wit, what we can be certain of is that the Constitution could have said "to promote Innovation in Science and useful Arts" — but it does not *by design*.[172]

But perhaps a second source of guidance might be found in the philosophy of progress from the Enlightenment. While multiple views of progress existed, the one that has perhaps best stood the test of time and perhaps resonated with at least some of the Framers is that of Immanuel Kant. Kant's first work considering progress was already published at the time of the drafting of the Constitution,[173] and we know that Kant's work was included in at least one Founder's library. [174] Both Kantian philosophy and the Framers' chosen words in Article I remind us that newer technologies are not necessarily better technologies.[175] In Kant's "anthropological"[176] view, progress is not predetermined or guaranteed; it is merely possible. When it happens, it is a product of the interaction of three elements: human psychology, reason, and institutions.[177] As explained by philosophers Agnes Tam and Margaret Meek Lange, Kant views the role of institutions as enabling progress, arguing for a federated approach of governance as most conducive to

[169] *See* JILL LEPORE, THESE TRUTHS: A HISTORY OF THE UNITED STATES 735–36 (2018).

[170] *Id.*

[171] *Id. See also Progress*, JOHNSON, *supra* note 167.

[172] *See id.*; *Innovation*, JOHNSON, *supra* note 168.

[173] Immanuel Kant, *Idea for a Universal History from a Cosmopolitan Point of View* (1784).

[174] We know Kant to have been read by at least one Founder. *See Thomas Jefferson Library Catalog*,
LIBRARYTHING, https://www.librarything.com/catalog.php?view=ThomasJefferson&deepsearch=kant. Kant's Idea for a Universal History from a Cosmopolitan Point of View was published in 1784. Thus, it is feasible that the Framers were aware of his work in progress.

[175] Thus, the Framers consciously avoided the word innovation but instead chose progress. The Constitution sets forth the Framer's goal "[t]o promote the progress of Science and useful Arts." U.S. CONST. art. I, § 8, cl. 8.

[176] "Put differently, a more accurate understanding of Kant's philosophy of progress is not metaphysical but anthropological. Contrary to Hegel, Kant is not trying to discover meaning or a specific trajectory from the actual course of history; rather, he wants to consider how human nature and agency have made possible the progressive trends in his own time." Agnes Tam & Margaret Meek Lange, *Progress*, STAN. ENCYCLOPEDIA PHIL. (Feb. 28, 2024), https://plato.stanford.edu/archives/spr2024/entries/progress/.

[177] *Id.*

peace, respecting that members are free and equal citizens. But "[t]he future of human history remains open." Thus, as explained by philosophers, Kant views progress as non-linear.[178]

Although still debated, Kant's view generally aligns with dominant views in modern philosophical approaches to "progress." [179] As conceptualized in modern philosophy, at least three different progress conversations are underway in our society — one is about scientific progress,[180] a second is about technological progress, and a third is about social progress.[181] Across this work, a distinction exists among descriptions of things that are merely new, and things that are "better." Progress implies the existence of a positive goal and movement forward toward it. In other words, "movement in the *wrong* direction does not constitute progress;" indeed, even scientific and technical inquiry of high precision and quality does not necessarily constitute progress.[182] Further, progress in science is a "goal-relative concept," which can be understood as "specifications of . . . epistemic utilities."[183] These utilities might include information verification and acquisition,[184] explanatory and predictive power,[185] or other values.[186] For purposes of a new approach to technology procurement animated in part by progress, this Essay argues that central considerations should include the nonlinear nature of

[178] *Id. See also* Sofie Møller, Kant on Non-Linear Progress, 23 ETHICS & POLITICS 127 (2021).

[179] Points of debate in modern discussions over progress include whether particular goals are accessible or utopian, whether particular goals are effectively recognizable, and whether criteria are backward-looking, forward-looking or a compromise. One example of an advocate of backward-looking criteria is Thomas Kuhn, known for his work on "paradigm shifts." Ilkka Niiniluoto, *Scientific Progress*, STAN. ENCYCLOPEDIA PHIL. (Jan. 22, 2024), https://plato.stanford.edu/archives/win2025/entries/scientific-progress/.

[180] "[T]he theory of scientific progress is not merely a descriptive account of the patterns of developments that science has in fact followed. Rather, it should give a specification of the values or aims that can be used as the constitutive criteria for 'good science.'" *Id.*

[181] "These types of progress have to be conceptually distinguished from advances in other human activities, even though it may turn out that scientific progress has at least some factual connections with technological progress (increased effectiveness of tools and techniques) and social progress (economic prosperity, quality of life, justice in society)." *Id.*

[182] "[I]t seems that there are no necessary connections between quality and progress in science." *Id.*

[183] *Id.* (citing ISAAC LEVI, GAMBLING WITH TRUTH: AN ESSAY ON THE INDUCTION AND THE AIMS OF SCIENCE (1973)).

[184] *Id.*

[185] *Id.* (citing CARL G. HEMPEL, ASPECTS OF SCIENTIFIC EXPLANATION AND OTHER ESSAYS IN THE PHILOSOPHY OF SCIENCE (1965)).

[186] For example, Thomas Kuhn's (1977) list of the values of science includes accuracy, consistency, scope, simplicity, and fruitfulness. *Id.*

technological advancement and the need for assessment of the mission efficacy and steps toward a recognizable progress goal.[187] The next section offers a model that considers these variables alongside resilience.

B. Shared Meta-Modeling in Procurement

Building on these two values of resilience and progress, the following section proposes a nested model for technology acquisition called the Procurement in Nested Technologies Model.

1. A Nested Model: PINT

Nested models, while perhaps somewhat novel in public policy contexts, have long been a mainstay in fields such as developmental psychology. Many of these models use a concentric circular design to demonstrate layering and dynamic processes, capturing change across time. One such model, the Bronfenbrenner ecological model consists of six concentric circles, each of which represents one level of social ecology.[188] The innermost concentric circle refers to the individual or child. This circle sits inside a slightly larger circle, the microsystem circle, which refers to the human's immediate environment, for example, a family unit. The microsystem sits inside the mesosystem circle, which involves connections across environments such as peer groups and communities. The mesosystem sits inside an exosystem circle, which refers to indirect environmental factors such as the technologies of the day that are developing independently of the internal layers to this point. The exosystem layer sits inside the macrosystem layer, which refers to societal level variables, such as law and political structures. All of these layers sit inside a chronosystem layer, which relates to change across time.[189]

[187] As explained by Niiniluoto, a "goal is *effectively recognizable* if there are routine or mechanical tests for showing that the goal has been reached or approached. If the defining criteria of progress are not recognizable in this strong sense, we have to distinguish true or *real progress* from our perceptions or *estimations of progress*." *Id.*

[188] BRONFENBRENNER, *supra* note 30, at 21–22.

[189] Philip A. Fisher & Joan Lombardi, *The New Ecology of Early Childhood: Revisiting Bronfenbrenner's Theory in the Context of Contemporary Challenges and Opportunities*, STANFORD CTR. ON EARLY CHILDHOOD, 3–4 (2025).

Borrowing the nested, concentric circle framing of the Bronfenbrenner model and other essential elements, we can build a nested model for technology procurement. This new nested model, PINT, allows for thinking through the impact of particular technologies on social and organizational resilience, on the one hand, and on advancing progress, on the other.

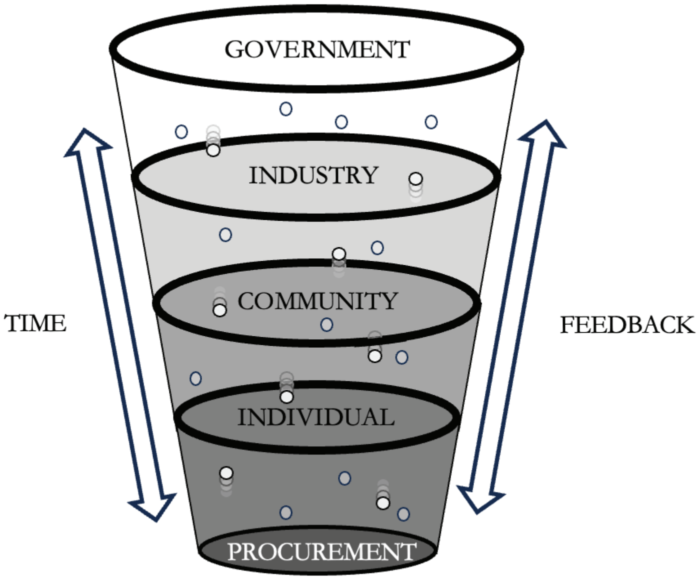

Figure 1: The Procurement in Nested Technologies ("PINT") model

The PINT model is expressly nonlinear in nature and dynamic, relying on feedback happening across any or all of the layers of the model at each point in time – *i.e.* any of the individual, community, industry, or governmental layers. Feedback may arise through formal channels set forth statutorily, agency rules, real time information from users, or technological change, such as the emergence of a security vulnerability that requires an immediate response. Included in the resilience analysis offered by PINT is a consideration of threat modeling and audit as well as the bounce back calculation previously described. In other words, the PINT model includes within it a type of threat meta-modeling exercise, mapping public and private sector procurement dynamics and their governance structures as experienced in practice. Traditional threat modeling methods familiar to technology professionals would be a component of the broader meta-modeling through PINT.[190]

Also included in PINT is a consideration of progress. The progress calculation is an assessment of the organization's broader mission and how the particular procurement advances a self-determined progress goal to further it (in a cost-effective manner). Note this is not an efficiency calculus using a "one-size-fits-all" economic cost analysis that ignores value in favor of low cost. Instead, this is a consideration of mission first, where cost-effective resource use is one part of that mission. The particular procurement is placed within the context of suitable, available options, where one option is stimulating novel approaches through less common methods of procurement where fit requires it. Specifically, using PINT the goal is to view procurement more broadly and creatively, engaging with suitable but less typical methods as needed. A more creative solution tailored to a context (and the most meaningful metrics within that particular context) is also often a cost-effective one. This mission-first model centers progress not only in outcome but also in choice of procurement method. It also recognizes that progress in procurement process can be emulated by later procurement scenarios, just as the procurement strategies employed by the agencies described in earlier sections of this Essay now provide a model for today's procurement. The PINT model assists in ensuring that decisions are placed in context of every level of nesting within society. In this way, a portion of irreparable harms might be avoided, and a set of broader implementation options aligned with organizational missions may be placed on the table for discussion.

2. An Implementation: A New Bureau of Technology Safety with a Pilot Projects Program

In other scholarship, this author has proposed the creation of a Bureau of Technology Safety (BoTS) in order to, among other things, assist existing agencies with troubleshooting problematic procurement situations.[191] The Bureau of Technology Safety or BoTS embodies three branches, one of which is dedicated to pilot projects, housing a team of technology experts that collaborate with the other two branches (enforcement and policy planning) as needed and with other governmental organizations and communities. This pilot projects branch

[190] For a discussion of threat modeling in information security see *The Ultimate Beginner's Guide to Threat Modeling*, SHOSTACK & ASSOCS., https://shostack.org/resources/threat-modeling (last visited Mar. 6, 2026).

[191] Matwyshyn, *Exploit Machina*, *supra* note 27.

would seek out opportunities across the federal government and in society to stimulate technology progress through, among other things, strategic collaborative procurement. Modeled in part on DARPA and ARPA-H, the BoTS pilot projects branch would importantly expand those approaches with light-touch collaboration inspired by the successes of the Electric Circus. Thus, BoTS pilot projects would seek to stimulate bottom-up technological progress in areas where the public and other agencies express the highest levels of social need (and where the private sector displays the least interest in successfully meeting those needs); BoTS would act as a supportive partner, providing resources, filling in knowledge gaps when they arise, and sharing expertise. The animating goal for these light-touch collaborations, as it was with the Electric Circus, would be helping organizations and communities that ask for assistance to arrive at their own hyper-local approaches most suitable for their contexts. A small BoTS "Tech Fair" team would then capture the tacit and contextual knowledge from these projects, turning them into models to share with future pilot project creators as potentially scalable and customizable approaches. BoTS' approach in its pilot projects branch would be predicated on the ideas embodied in the PINT model and in this Essay.

CONCLUSION

[T]his world of ours, ever growing smaller, must avoid becoming a community of dreadful fear and hate, and be, instead, a proud confederation of mutual trust and respect.

– President Dwight D. Eisenhower[192]

This Essay has offered a novel model for conceptualizing technology procurement, the PINT model, animated by goals of resiliency and progress. Embodying a nonlinear model, it is animated by concerns over evolving security threats and the trajectory toward human-machine symbiosis in procurement. One possible novel avenue for implementation of PINT would involve the creation of a pilot projects program within a new Bureau of Technology Safety.

This is the end, my friend. Thank you for calling.

– The Plague[193]

[192] *Eisenhower's Farewell Address*, *supra* note 1.

[193] HACKERS, *supra* note 2, at 1:30:30.