Closing the Software Understanding Gap

Publication: January 16, 2025

Cybersecurity and Infrastructure Security Agency
Defense Advanced Research Projects Agency
Office of the Under Secretary of Defense for Research and Engineering
National Security Agency

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

Summary

The widespread use of software that cannot be adequately characterized places society and government at unmeasurable risk. Software is embedded in countless systems responsible for providing U.S. critical infrastructure services that Americans rely on as well as systems providing national security capabilities. To maintain confidence in national security and critical infrastructure systems, mission owners and operators should be able to trust the system is functional, safe, and secure. The practice of constructing and assessing software-controlled systems to verify their functionality, safety, and security across all conditions (normal, abnormal, and hostile) is referred to as **software understanding**.

Today, mission owners and operators generally lack the adequate capacity for software understanding due, in part, to technology manufacturers *building* software that greatly outpaces their ability to *understand* it, creating a **software understanding gap**. This gap leads to an inability to create software that is secure by design, remediate defects once discovered, maintain software at the speed and scale of mission relevance, and secure software against exploits.

The software understanding gap arises from a disparity of technical investment: investment in software production has outstripped investment in improving understanding for decades. Where software understanding is concerned, strategic competitors—particularly the People's Republic of China (PRC)—are engaging in a technological arms race for preeminence. The PRC has achieved an elevated position through decisive national policy and sustained, multi-pronged investments in technology over the last decade to close their technology gap, enhancing not only their defensive capabilities but also their offensive capabilities to manipulate software and exploit vulnerabilities.

This report, coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), Defense Advanced Research Projects Agency (DARPA), the Office of the Under Secretary of Defense for Research and Engineering (OUSD R&E), and the National Security Agency (NSA)—hereafter referred to as the authoring agencies—is a call to action for the U.S. government to take decisive and coordinated action to close the software understanding gap. By closing the gap before other nations and obtaining a deep, scalable understanding of software-controlled systems, including artificial intelligence (AI)-based systems, the United States will secure an advantage in geopolitics for the foreseeable future and will help harden U.S. critical infrastructure from adversarial state-sponsored activity.

Software Understanding

Software-controlled systems are the foundation of U.S. critical infrastructure services and national security capabilities, and include software running on desktops, servers, information and communications technology (ICT) systems, AI systems, and operational technology components for systems such as:

- Military guidance systems (e.g., GPS, radar, and inertial guidance);
- Space systems (e.g., satellites, telescopes, and launch vehicles);
- Manufacturing systems (e.g., industrial control systems, digital twins, and computer numerical control (CNC) machines);
- Transportation systems (e.g., planes, trains, and automobiles); and
- Energy grid production systems (e.g., power plants, oil refineries, and wind turbines).

To engender high confidence in national security and critical infrastructure systems, mission owners and operators[1] must be able to routinely pose mission-related questions of these systems and receive thorough answers with the speed and confidence the mission demands. This is done via software understanding—the rigorous practice[2] of constructing and assessing software-controlled systems to verify their functionality, safety, and security by design across all conditions—normal, abnormal, and hostile.

The Software Understanding Gap

Today, mission owners and operators lack adequate capabilities for software understanding. These deficiencies stem from the **software understanding gap**—when technology manufacturers and developers *build* software that greatly outstrips their ability to *understand* it.

The outcome of this software understanding gap is an inability to effectively create software without defects, remediate them once discovered, maintain software at the speed and scale of mission relevance, and secure them against exploits. These types of outcomes are routinely seen in incidents of national significance, such as the 2021 pipeline disruption by ransomware, the 2021 Solar Winds Orion supply chain compromise, and Volt Typhoon's and Salt Typhoon's targeting of U.S. critical infrastructure and telecommunication systems.

The software understanding gap arises from a decades-long disparity of technical investment in software development capabilities unmatched by similar investments in understanding capabilities. The resulting software understanding gap is already extensive, as illustrated by the above cited incidents, and is advancing at an accelerating rate.

[1] Mission owners and operators include all government and industry actors who own and/or operate any national security or critical infrastructure system.

[2] This technical and rigorous practice encompasses multiple disciplines of the fields of science and engineering, including mathematics and logic. Examples of this include, but are not limited to, formal methods, artificial intelligence, threat modeling, game theory, and cognitive science.

The Prioritization Gap

U.S. strategic competitors are undertaking national policy measures, resulting in an unmatched software understanding advantage that provides them with more intimate knowledge of software than U.S. test and evaluation teams, program offices, and even system integrators. For instance, the Russian Federation has previously demanded access to software details in exchange for access to its markets.[3] Furthermore, the PRC has a robust policy and legal regime to reduce its dependency on foreign software that comprises its supply chain.[4] The PRC requires all software, foreign or domestic, that "might impact national security [to] undergo a national security review organized by the State,"[5] and requires all operators of critical infrastructure software systems to "provide technical support and assistance"[6] to the PRC.

These policies, when combined with significant investment in relevant technologies, set the stage for an aggressive race for dominance through software understanding.[7,8] Strategic competitor investments enhance their offensive capabilities to manipulate software, and they leverage their understanding of software properties to not only disrupt the intended functionality of targeted systems, but to co-opt these systems and use them as threat agents.

Mission Risk Impact

The software understanding gap results in significant risk to both critical infrastructure and national security systems. Ideally, all software behaviors that could jeopardize the system, whether inadvertent defects occurring during software manufacturing or supply chain compromises, would be identified and mitigated before placing mission software into service. Mission owners and operators perform extensive checks before deploying systems but insufficient software manufacturer understanding capabilities prevents adequate detection of such behaviors in a cost-effective and prompt fashion.

Without clear insight, inherent and residual risk—even potentially calamitous risk—is unknown. Lacking necessary technical capabilities, operators rely on attestations of secure development practices, software monitoring, and software bills of materials (SBOMs). While these current strategies have positive utility, they are unable to provide sufficient levels of assurance for national security and critical infrastructure systems.

---

[3] Iain Thomson, "Tech giants flash Russia their code blueprints in exchange for access." *The Register*, June 24, 2017, https://www.theregister.com/2017/06/24/tech_companies_show_russia_their_code/.

[4] PRC State Council, "Made in China 2025," translated by Etcetera Language Group, Inc. (Center for Security and Emerging Technology, 2022), https://cset.georgetown.edu/wp-content/uploads/t0432_made_in_china_2025_EN.pdf.

[5] PRC State Council, "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," Article 35 translated by Rogier Creemers, et al., *DigiChina*, June 29, 2018, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

[6] PRC State Council "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," Article 28 translated by Rogier Creemers, et al., *DigiChina*, June 29, 2018, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

[7] J.D. Work, "China Flaunts its Offensive Cyber Power." *War on the Rocks*, October 22, 2021, https://warontherocks.com/2021/10/china-flaunts-its-offensive-cyber-power/.

[8] Eugenio Benincasa, "From World Champions to State Assets: the Outsized Impact of a Few Chinese Hackers." *War on the Rocks*, September 3, 2024, https://warontherocks.com/2024/09/from-world-champions-to-state-assets-the-outsized-impact-of-a-few-chinese-hackers.

After software is in service, mission owners and operators spend significant resources upgrading and patching software to mitigate concerns once identified, including supply chain issues, risks to system availability, and exploitable vulnerabilities. Additionally, product components are often either vaguely specified or go unmentioned entirely by vendors, leading evaluators to skip examining critical items.

Third-Party Attestation

In furtherance of addressing these types of inherent software risks, the authoring agencies urge software manufacturers to include a trusted third-party attestation process into their Secure by Design program, and customers are encouraged to procure secure technology that has been certified by a trusted third-party attestation review process.

Critical Infrastructure (CI)

National Critical Functions (NCFs) are far too readily threatened or compromised, resulting in significant national impacts and enormous recovery costs.[9,10,11] Often accidental, such events include widespread outages in multiple CI sectors resulting from a flaw in a technology manufacturer's software,[12] cascading grid failure in the northeastern U.S. due to software flaws,[13] emergency services outages for 11 million people,[14] and numerous air- and space-craft failures—many leading to loss of life.[15,16,17]

Frequently, NCFs are at risk of malicious compromise because mission owners and operators lack the technical capability to adequately predict, prevent, and discover software issues in U.S. systems.[18] These risks are exemplified by several supply chain compromises, such as:

---

[9] U.S. Government Accountability Office. "High Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation," GAO-24-107231 (2024): https://www.gao.gov/assets/gao-24-107231.pdf.

[10] Chris Jaikaran, "Cybersecurity: Selected Cyberattacks, 2012-2022," *Congressional Research Service*, R46974 (2023): https://crsreports.congress.gov/product/pdf/R/R46974.

[11] Herb Krasner, et al., "The Cost of Poor Software Quality in the US: A 2022 Report," *Consortium for Information & Software Quality*, December 15, 2022, https://www.it-cisq.org/wp-content/uploads/sites/6/2022/11/CPSQ-Report-Nov-22-2.pdf.

[12] Clare Y. Cho, et al., "IT Disruptions from CrowdStrike's Update: Frequently Asked Questions," *Congressional Research Service*, R48135 (2024): https://crsreports.congress.gov/product/pdf/R/R48135.

[13] U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003, Blackout in the United States and Canada: Causes and Recommendations," *U.S. Department of Energy*, March 31, 2004, https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

[14] Colin Lecher, "The preventable coding error knocked out 911 service for millions," *The Verge*, October 20, 2014, https://www.theverge.com/2014/10/20/7014705/coding-error-911-fcc-washington.

[15] Samuel Gibbs, "Airbus issues software bug alert after fatal plane crash," *The Guardian*, May 20, 2015, https://www.theguardian.com/technology/2015/may/20/airbus-issues-alert-software-bug-fatal-plane-crash.

[16] Gregory Travis, "How the Boeing 737 Max Disaster Looks to a Software Developer," *Institute of Electrical and Electronics Engineers Spectrum*, April 18, 2019, https://spectrum.ieee.org/how-the-boeing-737-max-disaster-looks-to-a-software-developer.

[17] Lorraine Prokop, "Historical Aerospace Software Errors Categorized to Influence Fault Tolerance," *Institute of Electrical and Electronics Engineers*, March 2, 2024, https://ntrs.nasa.gov/api/citations/20230012909/downloads/Historical%20Aerospace%20Software%20Errors.pdf.

[18] Federal Bureau of Investigation Office of Public Affairs. "Director Wray's Opening Statement to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party," *Speeches*, January 31, 2024, https://www.fbi.gov/news/speeches/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party.

- WannaCry ransomware halting production of chips at the Taiwan Semiconductor Manufacturing Company Limited for several days in 2018 when a supplier introduced an infected tool;[19]
- The Russian Foreign Intelligence Service infiltrating SolarWinds in 2021;[20] and
- The compromise of a core library that underpins much of the internet's communication security in 2024.[21]

Notably, a congressional report found that the software systems controlling U.S. maritime ports "could, if desired, serve as a Trojan horse capable of helping the CCP and the PRC military exploit and manipulate U.S. maritime equipment and technology at their request."[22]

National Security

Every deterrent [23,24,25] capability the U.S. possesses, from conventional and nuclear forces to economic tariffs and sanctions, vitally depends on software. Software used in national security systems should function safely in all conditions; projecting global influence and engaging in compelling foreign policy actions depends on robust software executing its intended mission with a high level of confidence. As such, there is a compelling need for decisive and coordinated action to create the necessary software understanding capabilities.

On, Jan. 31, 2024, in his opening statement to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, FBI Director Christopher Wray stated:

> There has been far too little public focus on the fact that PRC [People's Republic of China] hackers are targeting our critical infrastructure—our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems—and the risk that poses to every American requires our attention now.
>
> China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities. If or when

[19] Mohit Kumar, "TSMC Chip Maker Blames WannaCry Malware for Production Halt," *The Hacker News*, August 7, 2018, https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html.

[20] Cybersecurity and Infrastructure Security Agency, "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," AA20-352A (2020): https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a.

[21] Jack Cable and Aeva Black, "Lessons from XZ Utils: Achieving a More Sustainable Open Source Ecosystem," *Cybersecurity and Infrastructure Security Agency*, April 12, 2024, https://www.cisa.gov/news-events/news/lessons-xz-utils-achieving-more-sustainable-open-source-ecosystem.

[22] Mark E. Green, et al., "Handling Our Cargo: How the People's Republic of China Invests Strategically in the U.S. Maritime Industry," *Select Committee on the CCP*, September 12, 2024, https://selectcommitteeontheccp.house.gov/media/reports/investigation-select-committee-ccp-house-homeland-finds-potential-threats-us-port.

[23] Chris Jaikaran, "Cybersecurity: Deterrence Policy," Congressional Research Service, R47011 (2022): https://crsreports.congress.gov/product/pdf/R/R47011.

[24] Chris Jaikaran, "The Cyberspace Solarium Commission: Illuminating Options for Layered Deterrence" Congressional Research Service (2020): https://crsreports.congress.gov/product/pdf/IF/IF11469#:~:text=In%20August%202018%2C%20Congress%20authorized%20the%20Cyberspace%20Solarium,Commission%20released%20its%20report%20on%20March%2011%2C%202020.

[25] Micharl J. Mazarr, "Understanding Deterrence" RAND Corporation (2018): https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.

> China decides the time has come to strike, they're not focused solely on political or military targets. We can see from where they position themselves, across civilian infrastructure, that low blows aren't just a possibility in the event of a conflict. Low blows against civilians are part of China's plan.[18]

Within the same session, CISA Director Jennifer Easterly remarked:

> Chinese cyber actors, including a group known as "Volt Typhoon," are burrowing deep into our critical infrastructure to be ready to launch destructive cyber-attacks in the event of a major crisis or conflict with the United States. This is a world where a major conflict halfway around the globe might well endanger the American people here at home through the disruption of our gas pipelines; the pollution of our water facilities; the severing of our telecommunications; the crippling of our transportation systems—all designed to incite chaos and panic across our country and deter our ability to marshal military might and citizen will.[26]

Previously undiscovered behavior in software has caused critical failures in aircraft, military systems, supply chains, and more—directly impacting national security objectives. In 2007, twelve F-22 Raptor planes deployed from Hawaii to Japan encountered an unexpected software condition that caused an on-board computer to crash as the planes were crossing the International Date Line. The incident caused the planes' critical systems to fail, including navigation, fuel, and communication components.[27] More recently, in 2022, the day after the full-scale Russian invasion of Ukraine, malicious cyber threat actors exploited thousands of satellite modems and erased their embedded software.[28] This both hampered the Ukrainian military's response to the invasion and caused malfunctions in 5,800 wind turbines in central Europe.[29]

In addition to these high-profile failures and attacks, gaps in software understanding lead to a false sense of confidence in national security systems. According to a U.S. government report, "in operational testing, [DoD] routinely found mission-critical cybersecurity vulnerabilities in systems under development" and, "due to limitations in the extent and sophistication of testing, [DoD] was likely aware of only a fraction of the total vulnerabilities in its weapon systems."[30] Moreover, "exercise authorities seldom permit warfighters to experience representative adversarial cyber effects because of the risk of degrading other training objectives. The net result of this limitation is a false sense of confidence by warfighters and

---

[26] Cybersecurity and Infrastructure Security Agency External Affairs. "Opening Statement by CISA Director Jen Easterly." *Blog*, January 31, 2024, https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly.

[27] David Cenciotti, "Crossing the International Date Line," *The Aviationist*, August 10, 2007, https://theaviationist.com/2007/08/10/crossing-the-international-date-line/.

[28] Foreign, Commonwealth, and Development Office and the Rt Hon Elizabeth Truss, "Russia behind cyber-attack with Europe-wide impact an hour before Ukraine Invasion," *Foreign Affairs Press Release*, May 10, 2022, https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion.

[29] Maria Sheahan, et al., "Satellite outage knocks out thousands of Enercon's wind turbines," *Reuters*, February 28, 2022, https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/.

[30] U.S. Government Accountability Office. "Weapon Systems Cybersecurity: Guidance Would Help DOD Programs Better Communicate Requirements to Contractors," GAO-21-179 (2021): https://www.gao.gov/assets/gao-21-179.pdf.

leadership alike."[31] Insufficient software understanding capabilities prevent the detection of such supply chain compromises before placing mission software into service.

Finally, the lack of software understanding degrades U.S. national security by preventing deployment of capabilities at the speed demanded by mission requirements. For example, DoD is expected to field new capabilities more rapidly but struggles to do so.[32] A significant part of this struggle is driven by the complexity of software and the processes to assure it, causing critical delays in operational capabilities.

Across NNSA's nuclear program, "[d]igital systems are increasingly being integrated into nuclear weapons and into activities and operations across the NNSA's nuclear security enterprise. There is potential for these digital systems to be hacked, corrupted, or subverted by malicious actors and NNSA has stated that securing its digital assets is an agency priority."[33] Additionally, many of the technical challenges U.S. Cyber Command faces involve methods of rapidly analyzing software and its functionality.[34] In contrast, the PRC has rapidly expanded and modernized both their conventional and nuclear capabilities.[35]

Economic

In 2022, the cost of defective software on the U.S. economy was estimated to be over $2 trillion USD.[11] This cost comprises operational failures, replacing legacy systems, identifying and fixing defects, addressing data breaches, and unsuccessful development projects. High-profile failures hinder substantial portions of the U.S. economy,[36] and can result in massive data breaches,[37] or force hundreds of organizations into costly remediation efforts.[38,39]

---

[31] U.S. Department of Defense. "FY2021 Annual Report," (Washington, DC, 2022), https://www.dote.osd.mil/Portals/97/pub/reports/FY2021/other/2021_DOTEAnnualReport.pdf?ver=YVOVPcF7Z5drzl8IGPSqJw%3d%3d.

[32] U.S. Government Accountability Office, "Weapon Systems Annual Assessment: DOD Is Not Yet Well-Positioned to Field Systems with Speed," GAO-24-206832 (2024): https://www.gao.gov/assets/gao-24-106831.pdf.

[33] U.S. Government Accountability Office, "Nuclear Weapons Cybersecurity: Status of NNSA's Inventory and Risk Assessment Efforts for Certain Systems," GAO-23-106309 (2023): https://www.gao.gov/products/gao-23-106309.

[34] U.S. Department of Defense, U.S. Cyber Command, "Technical Challenges Problems Guidance." USCC-J9-TO-2019-03-12 (2019): https://www.cybercom.mil/Portals/56/Documents/Technical%20Outreach/Technical%20Challenge%20Problems.pdf.

[35] Madelyn R. Creedon, et al., "America's Strategic Posture; The Final Report of the Congressional Commission on the Strategic Posture of the United States," *The Institute for Defense Analysis*, October 2023, https://www.ida.org/research-and-publications/publications/all/a/am/americas-strategic-posture.

[36] Office of Cybersecurity, Energy Security, and Emergency Response, "Colonial Pipeline Cyber Incident." U.S. Department of Energy (, 2021), https://www.energy.gov/ceser/colonial-pipeline-cyber-incident.

[37] U.S Government Accountability Office, "Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach," GAO-18-559 (2018), https://www.gao.gov/assets/gao-18-559.pdf.

[38] U.S. Government Accountability Office, "Federal Response to SolarWinds and Microsoft Exchange Incidents," GAO-22-104746 (2022): https://www.gao.gov/products/gao-22-104746.

[39] Cyber Safety Review Board, "Review of the December 2021 Log4j Event," *Cybersecurity and Infrastructure Security Agency*, July 11, 2022, https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf.

Further, $20 billion USD was committed by the U.S. government to replace the maritime port systems mentioned above,[40] while financial losses from a single technology manufacturer software crash were estimated at $15 billion USD.[41]

Future Vision

If software understanding challenges were addressed, mission owners and operators would have the ability to routinely ask mission-related questions of mission-relevant software and receive rigorous, reliable, rapid, and repeatable answers—during or after development. Further, this would provide mission owners and operators the ability to characterize mission risk from software based on technical evidence packages, prior to placing the software into service. In turn, this would usher justifiable confidence[42] in software across national security and critical infrastructure. Finally, this would enormously benefit the U.S. national economy, bringing down lifecycle costs of software while engendering confidence in critical applications, freeing up resources to strengthen national security and ensure economic prosperity.

This future is challenging but possible. The technologies needed to analyze software to prevent or discover undesirable behavior rest upon technical foundations with decades of progress, such as formal methods and AI. Recent breakthroughs provide new opportunities to rapidly advance software understanding capabilities. A radically improved future for software understanding and technically informed mission risk is possible, if the nation consciously decides to undertake and commit to the journey.

Current Efforts

The United States has engaged in several activities paving the way toward improving software understanding, including research investments, mission agency initiatives, and policy actions.

The National Science Foundation (NSF) has established the Secure and Trustworthy Cyberspace (SaTC) program and is partnering with the Department of Energy (DOE) to establish a new Correctness for Scientific Computing Systems (CS2) joint program.

Over the past twelve years, the Defense Advanced Research Projects Agency (DARPA) has initiated 10 programs related to mathematically provable methods supporting software understanding. These programs aim to demonstrate the viability of these approaches in mission systems. For more information, visit DARPA's webpage or listen to their podcast.

---

[40] White House Office of Public Engagement, "Fact Sheet: Biden-Harris Administration Announces Initiative to Bolster Cybersecurity of U.S. Ports," *Statements and Releases*, February 21, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/21/fact-sheet-biden-harris-administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports/.

[41] Carolyn Cohn, "Fortune 500 firms to see $5.4 billion in CrowdStrike losses, says insurer Parametrix," *Reuters*, July 4, 2024, https://www.reuters.com/technology/fortune-500-firms-see-54-bln-crowdstrike-losses-says-insurer-parametrix-2024-07-24/.

[42] U.S. National Institute of Standards and Technology, "Assessing Security and Privacy Controls in Information Systems and Organizations," NIST Special Publication 800-53A, Revision 5 (2022): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf.

Additionally, mission agencies have taken steps, with CISA launching the Secure by Design initiative and NNSA establishing the Nuclear Enterprise Assurance (NEA) program.[43]

The White House declared a national emergency arising from foreign adversarial threats to U.S. information and communications technology and services supply chains,[44] and encouraged software progress by publishing "Back to the Building Blocks," a technical report released in early 2024.[45]

More examples of U.S. software progress include the Office of Management and Budget adding formal methods and software understanding to national budget priorities[46] and the White House's call to incorporate several software understanding related priorities into the Federal Cybersecurity Research and Development Strategic Plan,[47] as well as calling for foundational improvements in understanding the safety, security, and trustworthiness of AI software.[48]

These policy actions help accelerate software understanding and provide the U.S. government with a strong foundation for establishing leadership in the pursuit.

Many mission-oriented agency activities effectively address some urgent needs, as well as mission-specific requirements, and are expected to continue. However, more robust understanding of software on a national scale requires strengthening its broad technical foundations. Additionally, while some activities are progressing specific elements of software understanding foundations, enhanced coordination is needed to identify common solutions that advance national capabilities more broadly and cost-effectively.

Given that numerous, key gaps in the foundational ability to proficiently articulate software understanding remain unfunded, the U.S.'s call for action has never been timelier.

Major technology manufacturers have found that, for select problems, rigorous software understanding capabilities can be an economical option that yields a positive return on investment.[49,50,51,52] These successes provide promising examples of technical foundations ripe for impactful application.

---

[43] National Nuclear Security Administration, "SD 452.4-1, Nuclear Enterprise Assurance (NEA)," SD 452.4-1 (2022): https://directives.nnsa.doe.gov/supplemental-directive/sd-0452-0004-1.

[44] Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," *The National Archives*, May 15, 2019, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[45] Office of the National Cyber Director, "Back to the Building Blocks: A Path Toward Secure and Measurable Software," *The White House* (2024), https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf.

[46] Shalanda D. Young and Harry Coker, Jr., "Administration Cybersecurity Priorities for FY 2026 Budget," *Executive Office of the President*, M-24-14 (2024): https://www.whitehouse.gov/wp-content/uploads/2024/07/FY26-Cybersecurity-Priorities-Memo_Signed.pdf.

[47] National Science and Technology Council, "Federal Cybersecurity Research and Development Strategic Plan," The White House (2023), https://www.whitehouse.gov/wp-content/uploads/2024/01/Federal-Cybersecurity-RD-Strategic-Plan-2023.pdf.

[48] White House Office of Public Engagement, "Memorandum on Advancing the United States' Leadership in Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence," *Presidential Actions*, October 24, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/.

[49] "facebook / infer," Meta, https://github.com/facebook/infer.

[50] "project-oak / oak," Google, https://github.com/project-oak/oak.

[51] "awslabs / aws-lc-verification," Amazon, https://github.com/awslabs/aws-lc-verification.

[52] "Z3Prover / z3," Microsoft, https://github.com/Z3Prover/z3.

Still, current industry efforts do not fully address their own needs and fall far short of meeting the broader needs of the U.S. government. Existing market incentives are insufficient to drive creation of the software understanding capabilities necessary for high confidence in the nation's national security and critical infrastructure missions.

A Call to Action

Closing the software understanding gap requires decisive and coordinated action across the U.S. Government. The challenge must be addressed through policy action, mission engagement, and technical innovation. Like previous national efforts to meet enormous challenges—the Manhattan project, the space race, and the war on cancer—addressing the software understanding gap requires effective organizational structures, subject matter expert-guided research direction, and an enduring and tenacious focus to address this urgent need.

Enduring national attention is necessary to enable a whole-of-government approach to national security and critical infrastructure missions to address associated policy and technical and resource challenges.

Policy

Policy should be broadly reconsidered to accelerate the development and adoption of software understanding capabilities and cultivate software understanding as a critical national resource.

Technology Procurement

As capabilities for software understanding continue to advance, it is essential to reimagine the associated acquisition policy. A transformative approach is needed that will empower the U.S. government to foster and incentivize the widespread adoption of ever-advancing capabilities, driving mission risk lower.

Legal Requirements

Legal and policy obstacles prevent mission owners and operators from deeply understanding the software, especially supply chain software, on which they depend—putting their missions at asymmetric risk to countries without such obstacles.

Evolving Threat Environments

The threat environment in which our critical national systems operate is highly dynamic and rapidly evolving. Any static statement of security requirements is likely to be quickly out of date. Software is currently deployed without adequate understanding of its behavior, introducing unknown risks into critical mission environments. As technical capabilities mature, policy will need to evolve, requiring and formalizing processes for adequately characterizing software behavior *before* introducing it into critical systems. Finally, current policies result in duplicative and wasted effort by inadvertently inhibiting sharing of existing tools and techniques.[53]

[53] D. Ghormley, et al., "The National Need for Software Understanding," *Sandia National Laboratories*, January 17, 2024.

Technical Solutions

The U.S. government can provide (1) the coordination and leadership needed to develop the technical capabilities for measuring software and (2) rationale as to how software behavior may pose a risk to NS&CI missions.[54] Such capabilities will involve the creation of foundational and applied research and development efforts.

In addition, the development of these software understanding capabilities includes new standards for reusable software understanding tools, secure code libraries, and interchangeable data. The creation of rigorous threat models will supply a mechanism to define and characterize the inherent risk of software, including emergent behaviors.

All suitable techniques (including formal methods, AI, and others) must be leveraged to develop rigorous, reliable, rapid, and inexpensive capabilities. These types of technical solutions will enable technology manufacturers and the U.S. government to reduce risk in newly created software and analyze risk in legacy and third-party software, including software supply chains.

Resourcing

Expanded and sustained investments in research, engineering, and support are necessary[55] to create the foundations for a unified set of software understanding capabilities that can be leveraged across missions, departments, and agencies. Public-private partnerships should be explored with experts from both sectors to ensure practical, cost-effective solutions that will work effectively given the size, complexity, and diversity of modern software systems. It is also essential to establish international partnerships, create academic centers of excellence, expand university curricula, and develop talent pipelines to create and leverage advancing software understanding capabilities.

Conclusion

The current and accelerating software understanding gap results in significant risk to both critical infrastructure and national security systems. Through decisive and coordinated action, the United States can reduce risk to these systems by closing the software understanding gap. Enduring attention is required to identify key gaps, establish and maintain a research-development-and-engineering roadmap, direct new research, align existing funding, and cultivate an innovative community for software understanding. By closing the gap before other nations and obtaining a deep, scalable understanding of software-controlled systems, including AI-based systems, the United States will secure an advantage in geopolitics for the foreseeable future and will help harden U.S. critical infrastructure against state-sponsored activity.

---

[54] Office of the National Cyber Director, “Back to the Building Blocks: A Path Toward Secure and Measurable Software,” Office of the National Cyber Director (2024), https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf.

[55] The CHIPS and Science Act provided $11B USD R&D funding for digital hardware and $39B USD in incentives for facilities and equipment. Similar levels of investment are needed for digital software. See Chips For America.

Disclaimer

The information in this report is being provided “as is” for informational purposes only. CISA, OUSD R&E, DARPA, and NSA do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA and co-sealers.

Acknowledgements

The National Nuclear Security Administration (NNSA) contributed to this guidance.