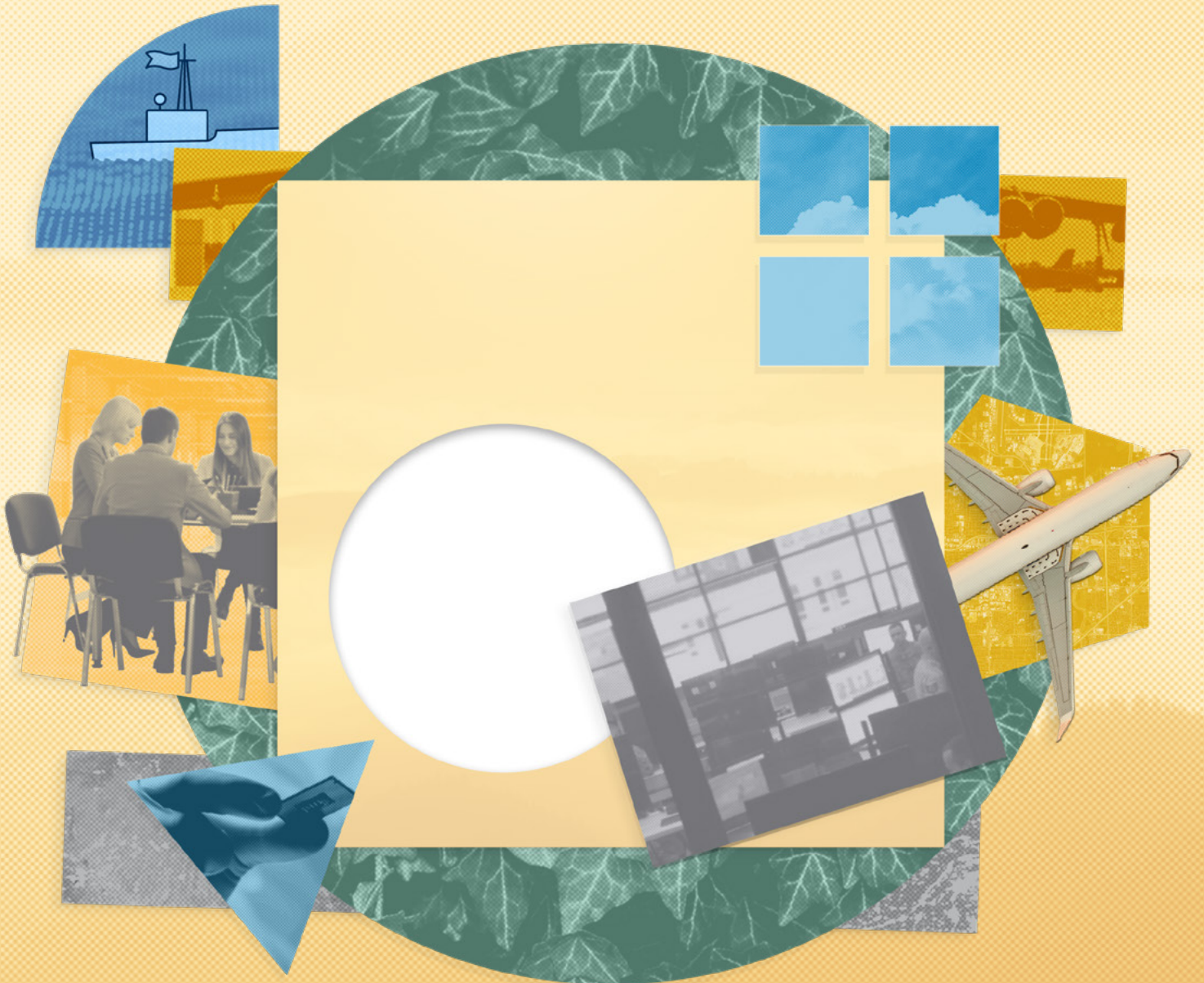


2

YEAR *in*
REVIEW



2022

Always focused on the future, the Software Engineering Institute (SEI) advances software as a strategic advantage for national security. We lead research and direct transition of software engineering, cybersecurity, and artificial intelligence technologies at the intersection of academia, industry, and government. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and are based at Carnegie Mellon University (CMU), a global research university annually rated among the best for its programs in computer science and engineering.

The *2022 SEI Year in Review* highlights the work of the institute undertaken during the fiscal year spanning October 1, 2021, to September 30, 2022.



“We remain consistent in our mission focus to trigger and enable transformational impact for our sponsor.”

A MESSAGE FROM THE DIRECTOR AND CHIEF EXECUTIVE OFFICER

For our nation’s defense and national security organizations, disruptive technology events and circumstances abound, such as technology advancements and new regulatory mandates. The mission of the Carnegie Mellon University Software Engineering Institute is to spur transformational impact for our sponsor, the Department of Defense, in the midst of those disruptions.

At the SEI, our people always seek ways to fulfill our mission. When the DoD recognized the threat of cyber intrusion as a present danger, for instance, the SEI brought together a community to build the discipline of cybersecurity engineering, which has transformed the way software is acquired, operated, and protected. To give the DoD confidence in its mission-critical systems, the SEI created and transitioned software architecture practices. Today, as advances in data management and computing power enable a greater role for artificial intelligence, the SEI leads a nationwide effort to form an AI engineering discipline to build and use AI-enabled systems that are robust and secure, scalable, and human centered.

Our story continues to be written because everyone at the SEI is committed to shaping the future of software. For example, our Safety Analysis and Fault Detection

Isolation and Recovery Synthesis research project (p. 22) is producing the means for future weapon systems to detect failures, recover from their effects, and reconfigure to adapt to new situations—all without human intervention.

In addition, our ongoing work to enable the evaluation of aerial object detectors that incorporate machine learning (p. 18) and with the U.S. Air Force Long-Range Standoff weapon (p. 14) are other examples of how we catalyze transformational change.

We remain consistent in our mission focus to trigger and enable transformational impact for our sponsor. We work in collaboration with researchers at CMU and other universities; in combination with customers in all service branches and many federal agencies; through leadership positions in the world’s foremost software engineering professional societies; and with the strength of a work culture and environment that cultivates and grows diversity, equity, and inclusion.

A handwritten signature in black ink, appearing to read "Paul Nielsen". The signature is fluid and cursive.

Paul Nielsen

EXECUTION STRATEGY

The SEI facilitates the transfer of research results to practice in Department of Defense (DoD) programs, the Office of the Secretary of Defense’s science and technology initiatives, and non-DoD U.S. government organizations where improvements will also benefit the DoD. In doing so, we gain deeper insight into mission needs—insight that forms the basis for new research. In addition, we transition matured technologies more broadly to Defense Industrial Base organizations and others in the DoD software supply chain.

We collaborate at the nexus of government, industry, and academia to integrate research in artificial intelligence, software, and cybersecurity to develop and pilot prototype tools, build and transition innovative solutions, and provide input for our sponsor’s policy decisions about software and related technologies. Through ongoing research and development and communication with customers, the SEI identifies priority areas for further research and development. Through our study approach, we generate academic and theoretical

reports, presentations, and books on gaps or issues in those areas. We make software tools, processes, data sets, analytic approaches, and training materials to mitigate those gaps or issues. We combine our body of knowledge with external material and systems engineering to deliver, through transition and transfer activities, quantitative impact to a U.S. government organization, DoD organization, or DoD end user.

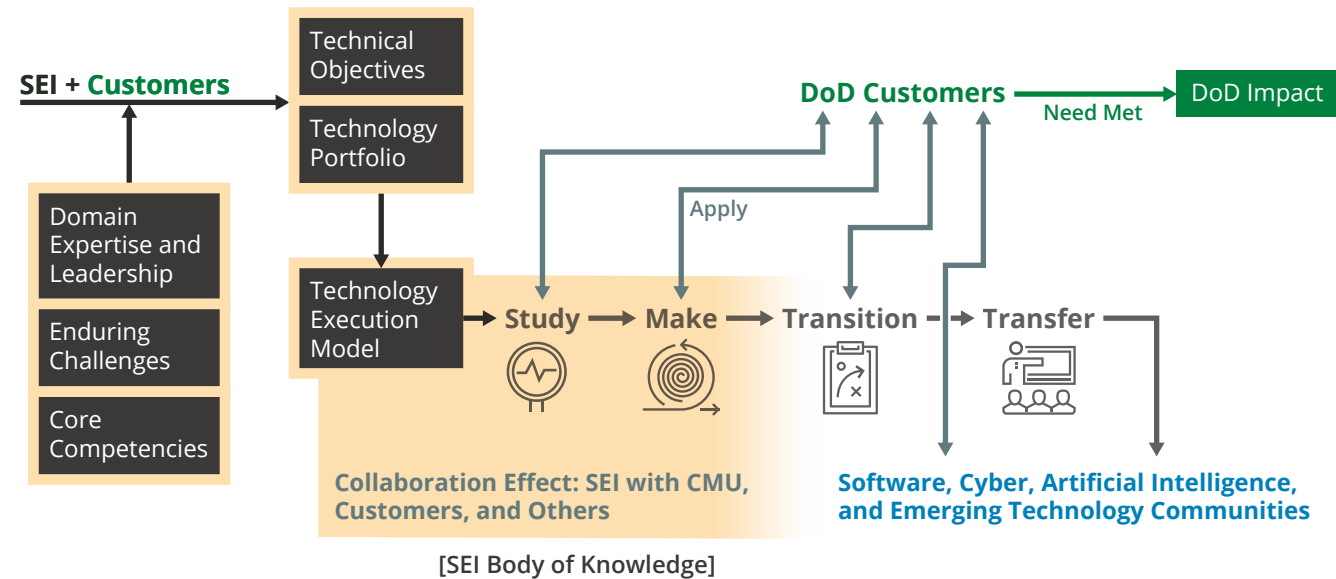
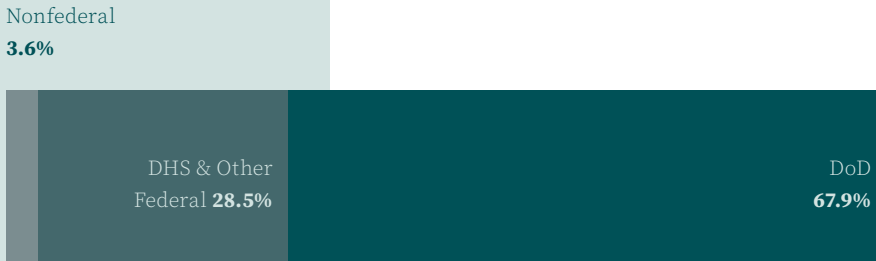


TABLE OF CONTENTS

- A Message from the Director and Chief Executive Officer 1
- Execution Strategy 2
- News Briefs 4
- The Drive Toward Stability 8
- Enabling Proactive Cyber Threat Detection in the Federal Civilian Executive Branch 10
- AI Engineering Symposium Assembles AI Community 11
- Collaborations Increase Impact 12
- Applying Causal Learning to Reduce Testing Times and Costs 13
- SEI Lends Expertise to Key Air Force Missile System Acquisition 14
- Keeping Ahead of Insider Risk 16
- Codifying Test and Evaluation of Machine-Learning Aerial Object Detectors 18
- Increasing American Competitiveness in Semiconductor Chips 21
- Assuring Increasingly Autonomous Cyber-Physical Systems 22
- Updated Energy Sector Cybersecurity Maturity Model Helps Keep the Lights On 24
- New Model Provides Blueprint for DevSecOps 26
- SEI Breadth and Depth Help DOT&E Adapt to Modern Software Development 28
- Leadership 30
- SEI Research Teams 34

Funding Sources

In fiscal year 2022, the SEI received funding from a variety of sources in the DoD, civil agencies, and industry.



NEWS BRIEFS

Implementing the National Agenda for Software Engineering

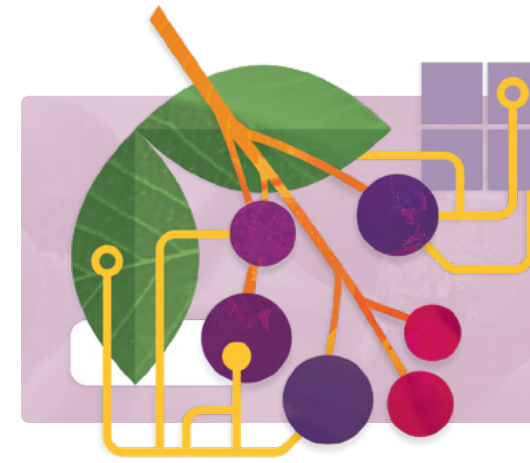
The SEI-led study *Architecting the Future of Software Engineering: A National Agenda for Software Engineering Research & Development* laid out a multiyear roadmap for engineering next-generation software-reliant systems. The SEI is leading technical engagements with the software engineering community to realize the roadmap's vision.

One of the roadmap's six focus areas, Assuring Continuously Evolving Software Systems, received support from the Federal Aviation Administration and Vanderbilt University in August 2022 when they and the SEI convened the Assurance Evidence for Continuously Evolving Real-Time Systems Workshop.

"The workshop gathered leading researchers, developers, and certifiers from across the industry, the Defense Department, and academia to work on two key issues in software assurance," said Dionisio de Niz, the SEI's technical director of assuring cyber-physical systems. "First, how can we automate the development and evaluation of assurance arguments to convince an oversight authority that a system is ready for fielding, using advances in formal methods to speed up the process, and how can we assure and reassure systems that include new algorithms or hardware, such as multicore processors?"

More technical engagements around the National Agenda for Software Engineering R&D are planned for 2023.

Get the study at sei.cmu.edu/go/nationalagenda.



"Very specialized semantics give users the knowledge of how these attacks are structured. These semantics are not available elsewhere."

ANDREW MELLINGER, Principal Engineer, SEI AI Division

Juneberry Version 0.5 Simulates Attacks on Machine-Learning Systems

Juneberry is an open source Python tool, created by the SEI's Artificial Intelligence (AI) Division, that verifies and validates machine-learning (ML) models by automatically training, evaluating, and comparing them against multiple data sets. The latest version of Juneberry adds the ability to

simulate attacks that could disrupt computer vision systems.

Property inference attacks reveal information about an ML system's training data. Using that information, attackers can craft and inject watermarks into image data to trick the ML system into unintended behavior.

Juneberry 0.5 allows users to prescribe ML model changes that simulate property inference attacks. "Very specialized semantics

give users the knowledge of how these attacks are structured," said principal engineer Andrew Mellinger. "These semantics are not available elsewhere."

The attack simulation capability will allow ML developers and researchers to test their models for weaknesses against property inference attacks and ultimately protect ML-powered image classification systems.

Explore Juneberry at github.com/cmu-sei/juneberry.

SEI Co-Authored Papers Awarded by International Conferences

Sharing research is key to the SEI's vision of shaping the future of software for a better world. In 2022, three papers co-authored by SEI staff were recognized for significant contributions to their fields.

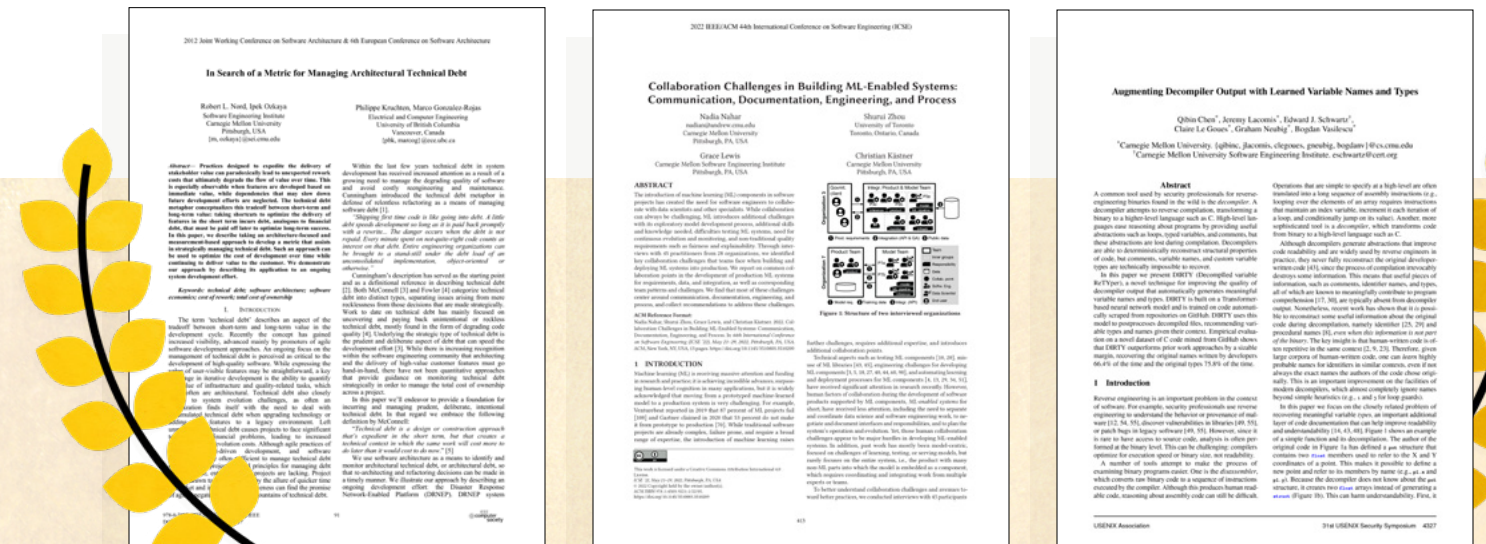
The 2012 paper *In Search of a Metric for Managing Architectural Debt*, by

Robert Nord and Ipek Ozkaya of the SEI, Philippe Kruchten, and Marco Gonzalez-Rojas, received the **Most Influential Paper Award** at the IEEE International Conference on Software Architecture for its lasting impact on software architecture research and practice.

Collaboration Challenges in Building ML-Enabled Systems: Communication, Documentation, Engineering, and Process, by Nadia Nahar, Shurui Zhou, Grace Lewis of the SEI, and Christian Kästner, won a

Distinguished Paper Award at the IEEE/ACM's 44th International Conference on Software Engineering (ICSE 2022).

Finally, *Augmenting Decompiler Output with Learned Variable Names and Types*, by Qibin Chen, Jeremy Lacomis, Edward Schwartz of the SEI, Claire Le Goues, Graham Neubig, and Bogdan Vasilescu, earned USENIX Security Symposium's Distinguished Paper Award for contributions to cybersecurity.



MORE NEWS BRIEFS



Implementing Responsible Artificial Intelligence

In 2021, the Defense Innovation Unit (DIU), which accelerates commercial technology adoption into the Department of Defense (DoD), published *Responsible Artificial Intelligence Guidelines in Practice*, co-authored by the SEI's Carol Smith and Alex Van Deusen.

DIU has since used the report to integrate the DoD's ethical principles for AI and its reliable, replicable, and scalable process into its commercial prototyping and acquisition programs and those of DoD customers. The report is also referenced in the DoD's *Responsible Artificial Intelligence Strategy and Implementation Pathway* toolkit.

Smith and Van Deusen have been educating DIU and other government teams on responsible artificial intelligence (RAI) and its real-world application by facilitating a series of workshops, giving presentations, and participating on DIU's behalf on national panel discussions. Smith continues to improve the report's processes, methods, and tools and to support DIU's RAI efforts.

For help with implementing RAI, contact the SEI AI Division at info@sei.cmu.edu.

Modernizing Land-Based U.S. Nuclear Deterrent

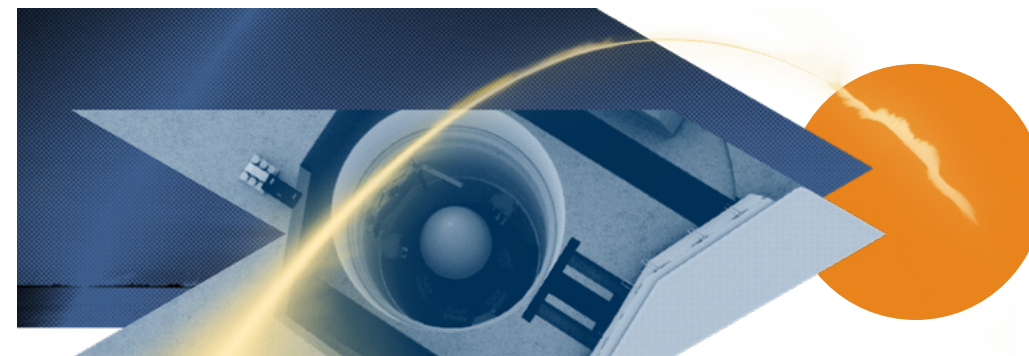
The SEI continues its work in software assurance and cybersecurity for the Sentinel program, the new and modernized land-based leg of the U.S. nuclear triad, formerly called the Ground-Based Strategic Deterrent system. In 2022, the technical team advanced its focus on delivering immediate, relevant impact.

The SEI team conducted an architecture evaluation that supports a continuous development cycle and analyzed software assurance to identify risks in not addressing cybersecurity early. Other contributions included groundwork for a software architecture office; formalizing enterprise Agile development processes within the program; improving software measurement, cost analytics, and estimation; workforce development on

many software development and acquisition topics; and a nuclear certification technical reference framework.

The Sentinel work also informed other SEI efforts on [technical debt](#), [zero trust](#), and [insider threat](#).

Activities in 2022 prepared Sentinel to understand and address continuous design to support the DevSecOps framework of continuous development, as well as address planning for software assurance and certification in the coming years.



“Organizations must continually assess risks in their changing threat environment and improve their zero trust implementations.”

TIM MORROW, Situational Awareness Technical Manager, SEI CERT Division

Zero Trust Industry Days Starts Critical Conversation

In August 2022, the SEI hosted the first *Zero Trust Industry Days* to encourage information sharing among organizations developing zero trust (ZT) solutions. “This event emphasized to organizations that adopting a zero trust strategy is not a one-time activity,” said Tim Morrow, the SEI's situational awareness technical manager. “Organizations must continually

assess risks in their changing threat environment and improve their zero trust implementations.”

The 2022 event focused on federal departments and agencies required to conform with two Office of Management and Budget (OMB) memoranda: [M-21-31](#) focuses on helping them reduce cybersecurity incidents, and [M-22-09](#) helps them move toward ZT cybersecurity principles.

More than 150 participants gathered, analyzed, and shared information

while 10 [vendors](#) recommended their ZT solutions. The event started a [critical conversation](#) between ZT researchers, vendors, and government bodies. Their collaboration expanded the ZT body of knowledge with papers on [best practices for implementation](#) and [future areas of research](#). Another ZT Industry Days event is tentatively planned for 2023.

Explore the SEI zero trust collection at resources.sei.cmu.edu/library/asset-view.cfm?assetid=888825.

The Drive Toward Stability

EDITORIAL Tom Longstaff

SEI chief technology officer Tom Longstaff describes the institute's technical strategy in the face of change.

Emerging disruptions to the field of software-intensive systems are of particular concern to the Department of Defense (DoD), which depends on software to deliver most new capabilities for maintaining strategic advantage. The SEI has reshaped its research strategy to take on emerging disruptions and integrated a number of research threads to multiply our impact.

Three disruptions have had the greatest impact on the DoD and our work. First, communications technology has enabled programs to interconnect directly, demanding an entirely new level of trust. Second, the interconnection of systems with multiple intersecting threads of execution, and the complex programs operating in these systems, present much larger attack surfaces. Third, the component pieces of **ultra-large-scale systems** are constantly evolving, increasing the danger of unintended consequences. All three disruptions can affect physical weapons and defensive systems. The result is an unstable environment with potentially devastating effects.

To stymie adversaries and create stability in the face of disruption, we revised the SEI's strategy in 2019. With our new strategic goal, *Software Transforming the Mission*, we sought to enable the DoD to realize advantage through software through four cross-cutting, targeted objectives. Three years after this adjustment, we have provided the DoD capable, timely, trustworthy, and affordable software and software research by pursuing four self-reinforcing objectives:

1. **Automate the software development and DoD acquisition lifecycle** with investments in cost estimation, automated trust assessment, and assuring software design is fully implemented through the development process.
2. **Create operational resilience for missions** with cyber threat hunting training, artificial intelligence (AI) decision support systems, AI robustness, and cyber-physical system assurance.

3. **Realize AI and future computing** with the development of an AI engineering discipline, data-intensive computing optimization, trustworthy and explainable AI, and quantum computing.
4. **Integrate the preceding objectives into mission-capable systems** that bring disciplined AI together with modern software development, cybersecurity, and architecture evolution.

To achieve these objectives, we transition research results to practice in DoD programs, the Office of the Secretary of Defense, and other U.S. government organizations. We also transition matured technologies to Defense Industrial Base organizations and others in the DoD software supply chain.

The SEI's applied research and advanced technology development (AR&D) aligns with DoD priorities and explores unexploited technologies and engagements. Field work with customers yields prototypes, practices, and pilots, and work with end users enhances SEI AR&D activities. We then generalize or scale AR&D prototypes or practices for the DoD and industry.

Our strategy of *Software Transforming the Mission* is effecting change in major government initiatives featured in this *Year in Review*. Our broad-ranging support of the Sentinel program (p. 7) has enhanced nuclear command, control, and communications (NC3). A new SEI network flow processor (p. 10) is transforming the threat hunting capability at the Cybersecurity and Infrastructure Security Agency (CISA). Our maturity modeling expertise (p. 24) informed major changes to the Department of Energy's Cybersecurity Capability Maturity Model (C2M2). Critical safety measures for the U.S. Air Force's Long-Range Standoff weapon (p. 14) are strengthening Joint All-Domain Command and Control (JADC2). The ultimate aim is to bring more stability and predictability to an ever-more-complex and disrupted software environment.



Enabling Proactive Cyber Threat Detection in the Federal Civilian Executive Branch

The Cybersecurity and Infrastructure Security Agency (CISA) is responsible for the cybersecurity of the [Federal Civilian Executive Branch \(FCEB\)](#), more than 100 agencies including every cabinet-level department but Defense. CISA analysts reactively query FCEB network records for past suspicious activity.

The recent [CISA Strategic Plan](#) calls for the agency to “continuously innovate our threat hunting capabilities to rapidly orchestrate threat identification and mitigation at scale.” To achieve this objective, CISA sought to identify suspicious network activity in the FCEB as it happens. But with limited staff and 100 billion new network flow records every day, the team needed automation to find the few suspicious signals.

In July 2022, the SEI’s CERT Division delivered to CISA the [Unexpected Outbound Protocols \(UNX-OBP\)](#) capability. This first-of-its-kind processor ingests native binary files from [SiLK \(System for Internet Level Knowledge\)](#), a CERT tool suite for capturing and analyzing network flow data, in CISA’s analytics environment.

CISA is currently testing UNX-OBP’s ability to find outbound network activity using the server message block (SMB) protocol. Because SMB is normally used to share files internally, outbound SMB traffic could signal data exfiltration. SMB is one of many protocols that the UNX-OBP processor could be extended to monitor for unusual activity.

The SEI’s knowledge of CISA’s mission and analytics environment, plus its familiarity with SiLK, enabled it to produce an efficient, low-cost, and easily integrated tool. The SEI is making this capability available as a NiFi processor for anyone to download. The processor has been observed in testing to ingest 98 billion flows per day in a single thread, filtering and enriching live, streaming data to a manageable number of alerts.

Automated cyber threat hunting is not new. But the UNX-OBP processor’s unique ability to do it at the scale of the FCEB will enable a sea change in CISA’s threat analytics, from reactive to proactive.

■ [Explore more CERT security tools at tools.netsa.cert.org.](#)

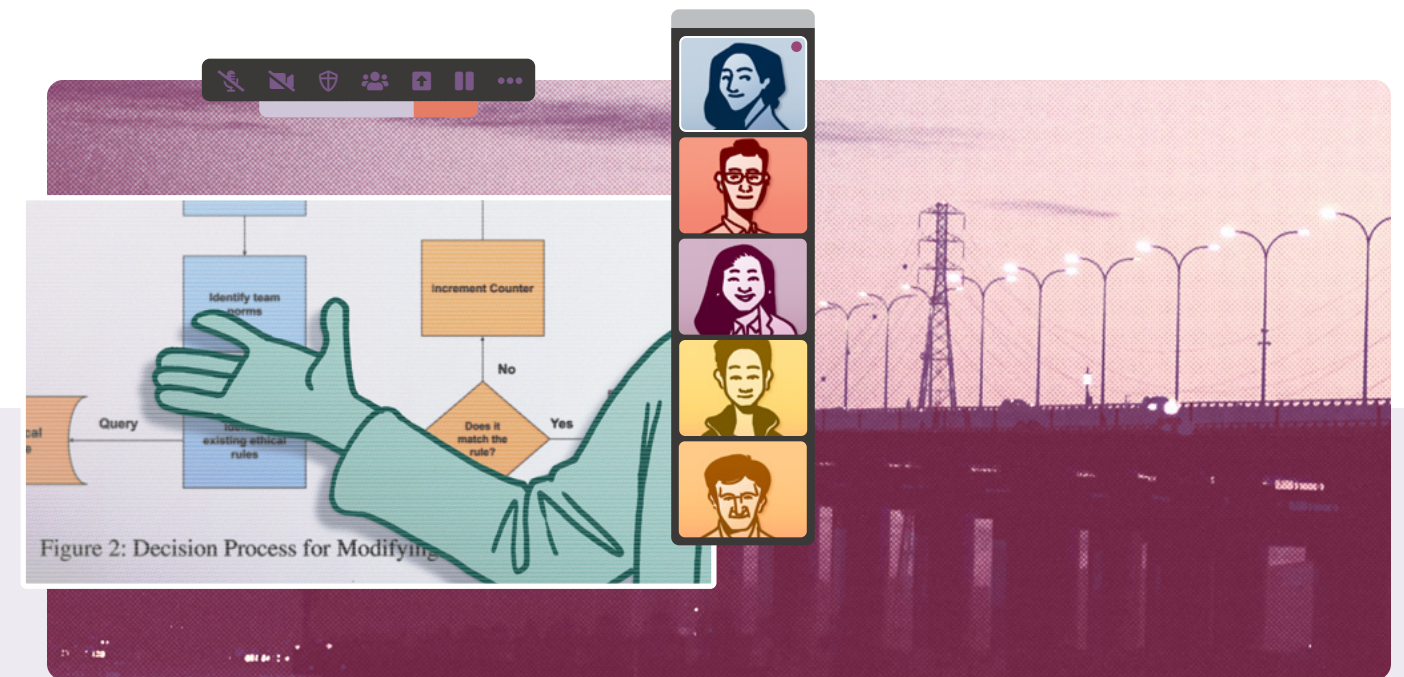
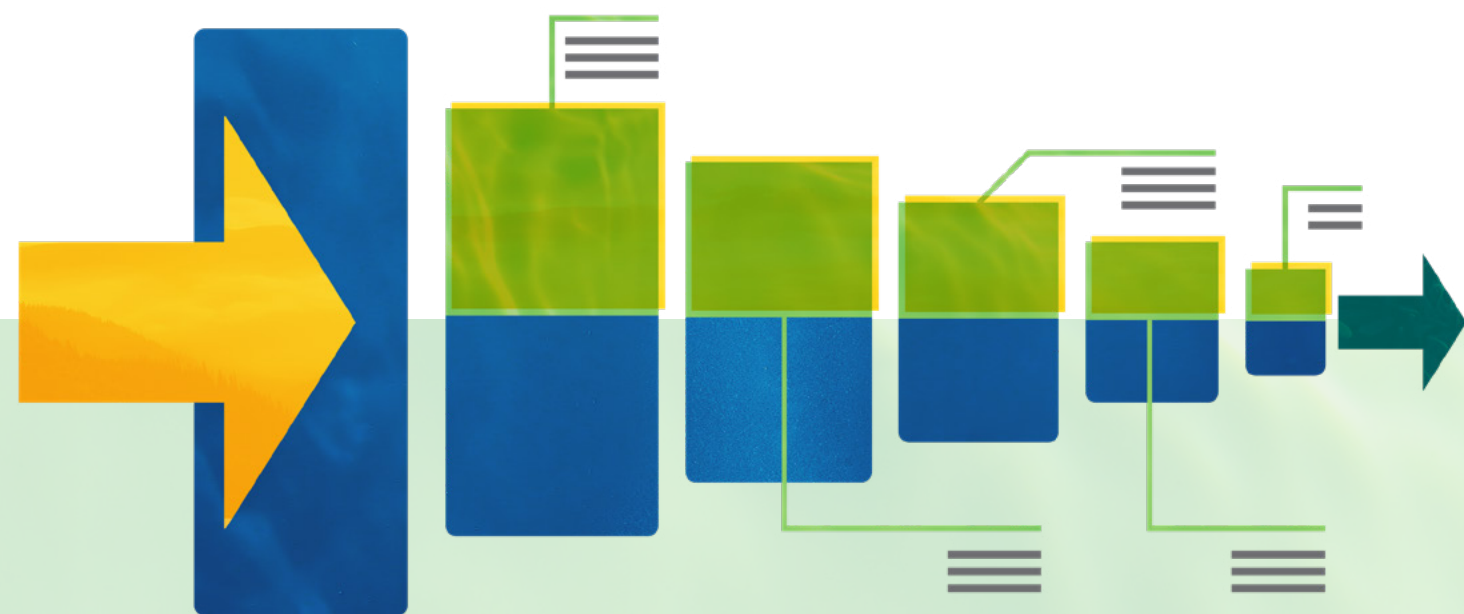


Figure 2: Decision Process for Modifying

AI Engineering Symposium Assembles AI Community

Formalized artificial intelligence (AI) engineering practices will help national defense and security agencies adopt AI in a way that is repeatable and scalable. As part of its efforts to grow the field of [AI engineering](#), the SEI is bringing together members of the AI community. The SEI, Duke University, SRI International, and MIT Lincoln Laboratory organized the [AI Engineering Symposium](#) in March 2022 for AI researchers and practitioners.

The symposium, part of the Association for the Advancement of Artificial Intelligence (AAAI) [Spring Symposium Series](#), focused on [human-centered](#), [scalable](#), and [robust and secure](#) AI. The symposium’s goal was to evolve the state of the art; foster critical relationships; and gather lessons learned, best practices, and workforce development needs in the area of AI engineering.

The AI Engineering Symposium drew participants from fields including robotics and computer science and from organizations including MIT Lincoln Laboratory, University of Maryland Applied Research Laboratory for Intelligence and Security (ARLIS), the Air Force Research Laboratory (AFRL), Clemson University, and Carnegie Mellon University. Representation from academia, industry, and the defense and national

security spheres enabled the kind of interactions needed for a cross-domain AI engineering discipline.

The event [proceedings](#) expand the AI engineering body of knowledge and practice with papers on adaptive autonomy, the DevOps lifecycle, human-AI interaction measurement, synthetic training images, hazard analysis processes, kernel density decision trees, human-AI teaming, and measuring beyond accuracy.

The SEI is leading a [National AI Engineering Initiative](#) with funding and guidance from the Office of the Director of National Intelligence (ODNI). AI engineering combines the principles of systems engineering, software engineering, computer science, and human-centered design to create AI systems in accordance with human needs for stakeholder outcomes. Events like the AI Engineering Symposium establish shared language across multidisciplinary researchers, outline the field’s progress and open questions, foster collaboration, and provide a forum to address the challenges of applying theoretical concepts in complex Department of Defense settings.

■ [Read the AI Engineering Symposium proceedings at resources.sei.cmu.edu/library/asset-view.cfm?assetid=884163.](#)

Collaborations Increase Impact

Succeeding through teamwork is a pillar of the [National Defense Science and Technology](#) strategy for the Department of Defense (DoD), announced in February 2022. The SEI joined its unique competencies in software, cybersecurity, and artificial intelligence with the expertise of other federally funded research and development centers (FFRDCs) and university affiliated research centers (UARCs) to solve a variety of technology problems in 2022 defense projects.

A collaboration with the Institute for Defense Analyses (IDA) helped the Office of the Director, Operational Test and Evaluation (DOT&E) research and analyze software and cybersecurity issues to support the DOT&E technical strategy.

In an ongoing partnership with MITRE, the SEI is conducting independent technical analyses (ITAs) of software efforts for the U.S. Air Force Platform One program and the Naval Information Warfare Systems Command (NAVWAR) Project Overmatch Technical Direction Activity (TDA). The SEI, MITRE, and the Aerospace Corporation conducted an ITA for Space Systems Command (SSC).

The Johns Hopkins University Applied Physics Laboratory and SEI are modeling the architecture and mission threads for an Integrated Warfighter Network (IWN) to support Joint All-Domain Command and Control (JADC2) initiatives for the U.S. Air Force Chief Architect Office.

These partnerships give the SEI a unique opportunity to integrate capabilities with another organization to advance the DoD's mission.



ALSO IN 2022, the SEI collaborated with

- the Aerospace Corporation to analyze different parts of a vendor's weapons system simulator (WSS) and provide a uniform list of enhancements to create an objective digital twin capability for the Air Force Long-Range Standoff (LRSO) System Program Office (SPO)
- MITRE to design and execute pilot programs to provide empirical information on software acquisition to programs and policy makers for the Office of the Deputy Assistant Secretary of Defense (DASD) for Acquisition Enablers (AE)
- MITRE to develop a DevSecOps pipeline that integrates programmable logic controller (PLC) development and automated testing capabilities for the Naval Sea Systems Command (NAVSEA) Program Executive Office (PEO) Aircraft Carriers

Applying Causal Learning to Reduce Testing Times and Costs

The Department of Defense (DoD) is focused on deploying the latest technologies more rapidly to make next-generation capabilities available to personnel in the field as quickly as possible. Many of these technologies require rigorous testing and evaluation involving live experiments in physical environments, which are often too costly and time consuming to sustain rapid development and deployment. One solution is to test with simulators, an environment whose realism the DoD is constantly seeking to improve.

The SEI is collaborating with the DoD's Director of Operational Test and Evaluation (DOT&E) and with the Naval Undersea Warfare Center (NUWC) on a novel approach to improve simulations for testing advanced systems. The SEI team is taking data from NUWC's in-water testing and comparing it to output from simulators using various methods, including multivariate outlier analysis. The technique identifies gaps—outliers in the combined data set—between simulations and real-world data.

“The novelty of our approach is to integrate multivariate outlier analysis with modern causal learning to create richer data for analysis,” explained Bob Stoddard, the SEI's project lead. Causal learning identifies direct causes of a particular outcome to make sense of a large

data set, in this case the interconnections between a weapon system, its environment, events that occur during testing, and the ultimate outcomes. A preliminary demonstration of causal learning on an NUWC in-water testing plan eliminated noncausal experimental factors, roughly doubling the test's efficiency.

Disciplines including medical research, economics, and social science already use causal learning. The SEI's work with DOT&E and NUWC is innovating the combination of this approach with outlier analysis to improve engineering testing and evaluation. This groundbreaking work is in its early stages, but it aims to give NUWC deeper insights into its in-water testing data to make more effective use of simulators, saving money and development time.

“The SEI's R&D into applying causal learning to discover differences between live test and simulation in support of model refinement represents a strong step toward achieving our goal of engendering a lifecycle approach to the verification and validation of modeling and simulation,” said Dr. Jeremy S. Werner, DOT&E chief scientist. “That includes a *live test, refine, predict* feedback loop to bring live data and simulation into increasing harmony over time.”



“The SEI's R&D into applying causal learning ... represents a strong step toward achieving our goal of engendering a lifecycle approach to the verification and validation of modeling and simulation.”

DR. JEREMY S. WERNER, Chief Scientist, DOT&E, Department of Defense

SEI Lends Expertise to Key Air Force Missile System Acquisition

Modernizing nuclear deterrence systems is a top priority of the 2022 U.S. National Defense Strategy. To support this strategy, the Air Force Long-Range Standoff (LRSO) System Program Office (SPO) is replacing the air-launched cruise missile inventory of the air-based leg of the nuclear triad.

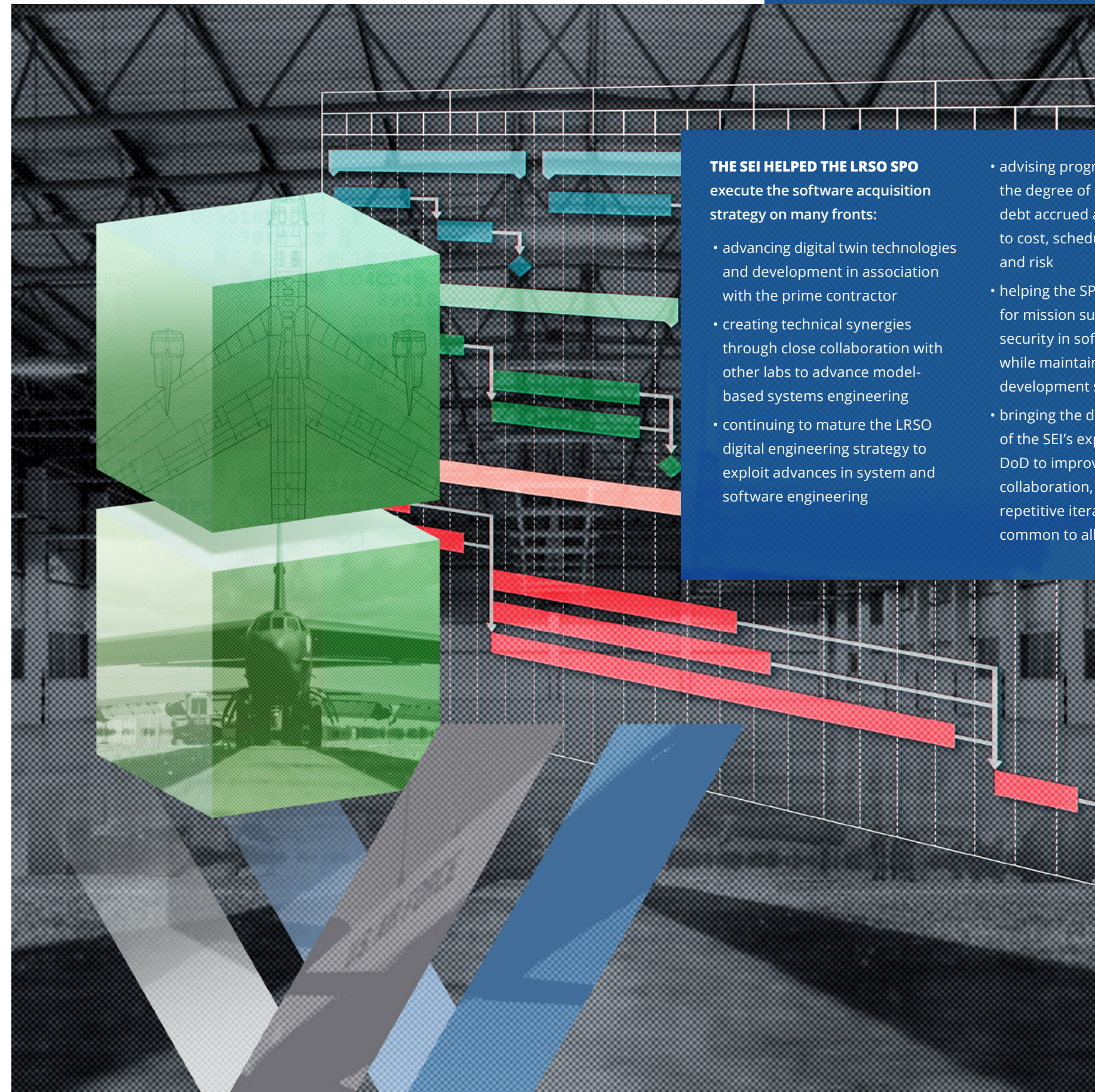
To navigate this complex acquisition, the LRSO SPO engaged the SEI to help it execute a software acquisition strategy that uses modern software development practices to reduce technical risk early in the Technology Maturation & Risk Reduction (TMRR) phase of the program. The LRSO SPO has also been working with the SEI to determine how and where to utilize innovations in platform cyber resiliency, automation, and best practices to meet new platform requirements while reducing projected lifecycle costs.

“The underlying theme for the support we’re providing the SPO is a determined focus on brilliance in the basics and fearless technical innovations that set this program up for success,” said the SEI’s [Stephen Beck](#), Advanced Deterrents Initiative lead. “We’re working closely with government stakeholders across the United States Air Force and engineers throughout the SPO to ensure that software and systems engineering are programmatically

optimized to reduce overall risk and to exploit opportunities.” With the SEI’s help, the program remains solidly on track to achieve initial operational capability (IOC).

Over the past fiscal year alone, SEI experts helped the SPO with a broad slate of software acquisition, engineering, and security tasks. They clarified and formalized the establishment of independent nuclear certification for advanced embedded weapon systems. They also established and exercised the engineering, architectural, and communication pathways for moving system nuclear certification forward to meet a demanding IOC date. Throughout the effort, they meticulously created and nurtured an enduring technical engagement culture with the principal developer, grounded in unimpeachable trust, software formalism, and disciplined engineering.

The SEI team’s depth of knowledge and commitment to the project enabled it to implement this robust program in a compressed time frame. “Though embedded within the LRSO SPO, I have ready access to expertise throughout the SEI,” noted David Walbeck, the SEI’s LRSO technical lead. “The software and systems engineering impacts our team has achieved, with a comparatively modest budget, have been dramatic.”



Keeping Ahead of Insider Risk

Some of the most damaging security incidents to organizations come from within. According to a 2020 Ponemon Institute study, 60 percent of organizations surveyed had at least 20 insider threat incidents per year, each costing an average of \$756,760. Public administration organizations are a fifth of insider victims.

The SEI released the seventh edition of the *Common Sense Guide to Mitigating Insider Threats* in September 2022. The CERT National Insider Threat Center updated the long-running guide to include a new best practice and a mapping to the National Institute of Standards and Technology (NIST) Privacy Framework.

The new edition comes at a time of change in the insider threat landscape. An increasingly fluid workforce, with many remote workers and a high resignation rate, has exacerbated risks to companies' confidential information. Federal agencies are being targeted with more and more misinformation or malinformation campaigns. These are just the latest changes the SEI's National Insider Threat Center has seen over the 20 years it has studied insider threat, helped hundreds of organizations build and evaluate their insider risk management programs, taught insider threat courses, and iterated the *Common Sense Guide*.



“We are transitioning the techniques we use to gather and analyze our [insider] incident corpus.”

DAN COSTA, Technical Manager, Enterprise Threat and Vulnerability Management, SEI CERT Division

The guide details 22 best practices that organizations can use to manage insider risk. The new best practice, “Learn from Past Insider Threat Incidents,” has guidance on developing and analyzing a repository of insider trends within an organization and its sector. “We see organizations not learning from institutional knowledge,” said Dan Costa, technical manager of the CERT Division’s Enterprise Threat and Vulnerability Management team. “With this best practice, we are transitioning the techniques we use to gather and analyze our incident corpus,” he said, referring to a CERT database drawn from public records of more than 3,000 insider threat incidents.

The practices are mapped to the CERT Resilience Management Model (CERT-RMM) and security and privacy standards, such as, among others, ISO/IEC 27002:2013, the NIST Cybersecurity Framework, and—new to this edition—the NIST Privacy Framework.

“Because our best practices encompass cybersecurity, information security, and operational resilience, it’s important to connect them to a broad array of standards so organizations can find the best guidance for their circumstances,” said Costa. The NIST Privacy Framework mapping helps organizations balance security with insider privacy as instantiated in the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

The *Common Sense Guide* takes a tool-agnostic approach that organizations can apply to any

insider monitoring solution. During insider threat vulnerability assessments, SEI experts work with an organization’s solution vendors. The vendors provide the raw tools and telemetry, and the SEI provides expertise on how incidents evolve, what defines normal activity, and how to refine sensors and analytics. The SEI’s final assessment report details the organization’s exposure to insider threats along multiple vectors, including technical, behavioral, process, and policy.

“We serve that gap-bridging role of a federally funded research and development center,” Costa said. “We know the technical capabilities, the government customer, and how to help the customer and their vendors communicate.”

Download the *Common Sense Guide* at resources.sei.cmu.edu/library/asset-view.cfm?assetid=886874.

Learn more about the SEI’s insider threat research at sei.cmu.edu/our-work/insider-threat.

Codifying Test and Evaluation of Machine-Learning Aerial Object Detectors

Aerial object detection provides critical information for domains ranging from agriculture to humanitarian and disaster relief, as well as intelligence, surveillance, and reconnaissance in the national security domain. Machine learning (ML) automatically processes the huge amount of data from aerial imagery and helps human analysts extract actionable information. However, ML-enabled object detection is a fast-changing field, and the test and evaluation of aerial object detectors has not kept pace. Determining which aerial object detectors yield accurate results is important for organizations seeking to develop, acquire, or deploy this technology.

Development of systems that incorporate machine-learned models as core components to analysts' workflows has been the research focus of Eric Heim, a senior research scientist in the SEI's Artificial Intelligence (AI) Division. He and his team have studied the many considerations necessary for such systems' design, production, and evaluation. In 2022, they completed the report *A Brief Introduction to the Evaluation of Learned Models for Aerial Object Detection*.

Evaluation covers the numerous decisions that go into training a detector, including the role of data, the choices involved in design, and the thresholds used to post-process outputs. Targeted evaluation involves experiments to measure the performance of detectors in specific ways to better inform stakeholders of how detectors behave in different settings. Because of the complexity of the object detection task and its intended environment of deployment, it is important to design evaluation procedures that provide test teams with quantifiable data reflecting specific performance characteristics.

Heim said that evaluation must focus on the requirements of the detector instead of the broad notions of performance typically seen in ML literature. "We focus on evaluation metrics, which are the computations used to measure the quality of a detector in a specific, quantifiable way. Each metric measures

different characteristics, so it is important to understand what they are measuring specifically and how that relates to important requirements. We concentrate on performance characteristics associated with the quality of the detectors' predictions."

The insights in the *Evaluation* report will be useful to organizations involved in aerial object detection. "The SEI is uniquely suited in that we have technical expertise on object detection, but we're also familiar with organizations in domains that perform aerial imaging," Heim said. "We're able to understand their problems in a way not available in the larger active community, and that allows us to provide assistance tailored to their specific mission space as opposed to object detection as a whole."

Though the report's scope is narrow, it answers calls from the defense sphere to strengthen AI test and evaluation techniques, as in the Defense Industrial Base report *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense*. Heim's research also seeks to make more **robust and secure AI**, one of the three pillars of AI engineering, to be applied to all AI-enabled Department of Defense acquisitions.

Download *A Brief Introduction to the Evaluation of Learned Models for Aerial Object Detection* at resources.sei.cmu.edu/library/asset-view.cfm?assetid=890521.



"The SEI is uniquely suited. We have technical expertise on object detection, but we're also familiar with organizations in domains that perform aerial imaging."

ERIC HEIM, Senior Research Scientist, SEI AI Division

Increasing American Competitiveness in Semiconductor Chips

The decline of U.S. semiconductor production and our reliance on nondomestic chips has sparked concerns about supply chain constraints and the potential insertion of vulnerabilities in chips during fabrication. Since before the [Creating Helpful Incentives to Produce Semiconductors \(CHIPS\)](#) and Science Act of 2022, the SEI has been helping the Department of Defense (DoD) boost U.S. competitiveness, innovation, and national security in semiconductor and microelectronics manufacturing.

The Defense Advanced Research Projects Agency (DARPA) invested \$1.5 billion in the Electronics Resurgence Initiative (ERI) to revive microelectronics production in the United States, decrease hardware design and manufacturing costs, and optimize hardware. In 2022, the SEI partnered with DARPA to support testing and evaluation in two ERI projects, [Data Protection in Virtual Environments \(DPRIVE\)](#) and [Domain-Specific Systems on Chip \(DSSoC\)](#).

Security and efficiency are at the heart of the work. DPRIVE's focus is on developing hardware accelerators that utilize novel hardware, software, and architectures to reduce the processing overhead required for fully homomorphic encryption (FHE) calculations, which enable computation on encrypted data. DPRIVE aims to make FHE a practical solution to ensure data security across the DoD. DSSoC is working to develop heterogeneous systems-on-chips (SoCs) to improve the performance of applications within various specific domains. The goal of these programs is to enable better hardware-software co-design through tool integrations that balance efficiency and flexibility. Multiple performers, or third-party organizations, are developing technology to advance both programs.

Evaluating these technologies is the SEI's role. The SEI has developed an evaluation methodology to make fair comparisons of newly designed technologies of varying maturity from multiple performers. To gauge system readiness, SEI researchers employ usability metrics to evaluate system maturity, code quality, and scalable software design. This flexible testing and evaluation

methodology focuses on identifying risks and providing feedback to performers and DARPA to maximize long-term success while they focus on pushing innovation on tight deadlines.


SEI researchers work directly with performers—each of which had upwards of \$10 million invested in them—to test and improve developed technology, with program managers to submit evaluations and recommendations, and with other DoD groups, such as the U.S. Army, to transition the technology into use. The SEI's technical work provided DARPA with data to help inform their decision on which performers to move forward from phase one to phase two of the DPRIVE program.

Researchers working on ERI programs require uniquely broad and deep skills and expertise. “You really have to have a deep knowledge of the full technology stack, what I like to call algorithms to assembler,” explained John Wohlbiel, a senior research scientist and Advanced Computing Lab lead in the SEI's AI Division. The expertise of SEI researchers spans algorithms, high-level programming languages, compiler technologies, low-level language concepts, and hardware.

This deep knowledge, combined with the SEI's status as a federally funded research and development center, has given the SEI a unique value proposition. “We serve as expert first users and provide an unbiased evaluation of the technology,” Wohlbiel said.

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions, and/or findings expressed are those of the author(s) and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Distribution Statement 'A' (Approved for Public Release, Distribution Unlimited)



“We serve as expert first users and provide an unbiased evaluation of the technology.”

JOHN WOHLBIEL, Senior Research Scientist and Advanced Computing Lab Lead, SEI AI Division



“The challenge is in managing a double layer of complexity to capture complex phenomena at both the physics and cyber levels.”

JEROME HUGUES, Senior Architecture Researcher, SEI Software Solutions Division

Assuring Increasingly Autonomous Cyber-Physical Systems

The 2018 Department of Defense (DoD) Artificial Intelligence (AI) Strategy touts AI as a potentially game-changing opportunity to improve its autonomous systems. The integration of AI has significantly enhanced the capability of cyber-physical systems (CPSs) to provide advanced control, situational awareness, and autonomy. These advances also make it harder to assure systems. Understanding the impact of AI functions on system safety requires a fine understanding of system architecture. In the Safety Analysis and Fault Detection Isolation and Recovery Synthesis (SAFIR) project, SEI researchers are collaborating with academia to develop tools and a body of knowledge to analyze the impact of AI functions on the assurance of safety-critical systems.

The growing complexity of CPSs has led to more autonomous features being added to systems such as vehicles and factories. These increasingly autonomous

cyber-physical systems (IA-CPSs) layer hardware, AI-enabled functions or decision-making processes, human operators, and software in a complex architecture. They not only must detect failures and recover quickly but also continuously reconfigure and autonomously adapt to different situations without human intervention to prevent potentially fatal incidents.

SAFIR aims to ensure that IA-CPSs properly detect and mitigate any errors before they threaten the system. “The challenge is in managing a double layer of complexity to capture complex phenomena at both the physics and cyber levels,” explained Jerome Hugues, an SEI senior architecture researcher. Just as a thermometer needs a moment to adjust to changing temperatures, an AI-powered, unmanned aerial vehicle (UAV) needs time to sense, process, and react to ongoing physical actions. The cyber platform driving autonomy

functions must anticipate potential problems and balance physical processes.

SEI and Georgia Tech researchers defined a decision procedure for selecting the most appropriate detection and mitigation strategies for a broad set of faults or attacks on IA-CPSs. They built the procedure by systematically analyzing the large body of knowledge on fault detection mechanisms, both traditional statistical techniques and others that use reinforcement learning, a machine-learning technique. The resulting fault taxonomy includes guidelines for selecting the published fault detection techniques most relevant to the system’s operational context.

The SEI, along with Kansas State University and industry partners Galois and Adventium Labs, then mechanized the linguistic semantics of architectural descriptions in the Architecture Analysis and Design Language (AADL) standard. This mathematically grounded definition of AADL, available on GitHub as [Oqarina](#), allows for more precise simulation and reasoning capabilities for the language. AADL is part of many embedded

systems, including DoD projects such as [Future Vertical Lift](#). SAFIR research also produced the [Architecture-Supported Audit Processor \(ASAP\)](#), a representation of safety argumentation for review by certification authorities. AADL semantic mechanization sets the foundation for the semantic mechanization of IA-CPS architectures, which will guarantee the proper mitigation of faults, down to the implementation.

The work also informed updates to AADL version 2.3 as well as academic and industry projects for the [Defense Advanced Research Projects Agency \(DARPA\)](#) and the U.S. Army’s [Grand Unified Modeling of Behavioral Operators \(GUMBO\)](#) program. “We have delivered a large body of research, including scientific papers supported by software tools, that provides a foundation for the academic community and industry,” noted Hugues.

Ultimately, SAFIR’s advancements in IA-CPS fault mitigation will bring the DoD’s vision of safer AI systems a step closer.

Learn more about SAFIR at resources.sei.cmu.edu/library/asset-view.cfm?assetid=889318.

Updated Energy Sector Cybersecurity Maturity Model Helps Keep the Lights On

Advances in technology, such as distributed energy resources, are increasing the amount of communication between devices that enable safe, reliable delivery of energy to consumers. At the same time, adversaries of the United States are increasingly targeting [cyber attacks on critical infrastructure](#).

A 2011 White House initiative tasked the Department of Energy (DOE) to create a more comprehensive, consistent approach to measuring the security posture of the energy sector. The DOE formed a working group of research organizations, including the SEI, and energy sector stakeholders. In just five months, the public-private partnership with the energy industry produced the [Cybersecurity Capability Maturity Model \(C2M2\)](#), which received a major update in 2022.

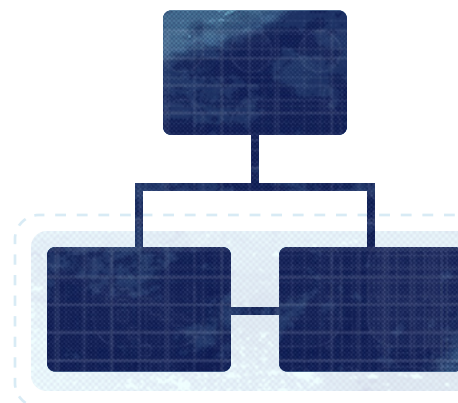
The 2012 model gathered more than 350 cybersecurity practices, grouped into objectives across 10 domains—logical groupings of cybersecurity practices. The practices are organized by three progressive maturity levels referred to as the Maturity Indicator Levels (MILs). Voluntary C2M2 self-evaluations give utilities, from small municipals to large investor-owned enterprises, a snapshot of their cybersecurity posture they can use to evaluate their capabilities, identify gaps, prioritize improvements, and track progress over time.

“A consensus cybersecurity measurement had to come from the energy industry, but we needed a carefully architected maturity model,” said Fowad Muneer, acting deputy director of Risk Management Tools and Technologies within the DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER). The SEI had decades of experience in developing maturity models, such as the foundational [CERT Resilience Management Model \(CERT-RMM\)](#), which became the starting point for the C2M2.

Since 2012, cyber attacks on energy resources, such as the 2021 [ransomware attack](#) on Colonial Pipeline, have become more sophisticated. Other changes in the cybersecurity landscape, including zero trust principles and artificial intelligence, as well as multiple new executive orders on [cybersecurity](#) and [critical infrastructure](#), spurred the DOE to update the C2M2.

The DOE assembled a project team, which included the SEI, that collaborated with [145 cybersecurity experts from 77 energy sector and cybersecurity organizations](#) on C2M2 revisions over three years.

After addressing public comments, reviewing the model for technological currency, and piloting it with energy companies, the DOE published C2M2 version 2.1 in June 2022. “We scrubbed the model end to end, looking for



blind spots,” said CESER’s Muneer. “That gives us confidence that this is a robust model for today’s threats and technology landscape.”

The update revised two-thirds of the practices and merged the previously separate models for the electricity subsector and oil and natural gas subsector. A Cybersecurity Architecture domain was added, and the Third-Party Risk Management domain was refreshed to reflect increasing supply chain cybersecurity risks. The update also more closely aligns the model’s practices with the [NIST Cybersecurity Framework \(CSF\)](#).

In each of the seven months following the release of C2M2 version 2.1, an average of more than 2,500 unique users accessed the [HTML-based C2M2 tools](#). This interest builds on the popularity of the HTML and PDF formats of the earlier C2M2 versions, which had been requested thousands of times since 2012.

“The updates and improvements to the C2M2 model represent significant collaborative efforts between industry and our government partners to address the challenges of an evolving threat landscape,” said Kaitlin Brennan, director of cyber and infrastructure security at Edison Electric Institute, an industry group involved in the C2M2. “They further strengthen our collective cybersecurity programs and operational resilience.”

Photo U.S. Department of Energy



“We scrubbed the model end to end, looking for blind spots. That gives us confidence that this is a robust model for today’s threats and technology landscape.”

FOWAD MUNEEER, Acting Deputy Director, Risk Management Tools and Technologies Division, CESER, Department of Energy

New Model Provides Blueprint for DevSecOps

Adopting DevSecOps methods is challenging for large Department of Defense (DoD) software acquisition and development groups. While policies such as the [software acquisition pathway](#) encourage government programs to use DevSecOps and Agile methods, they do not say how. The DevSecOps literature is too broad to be practical, and DevSecOps tools are too narrowly scoped.

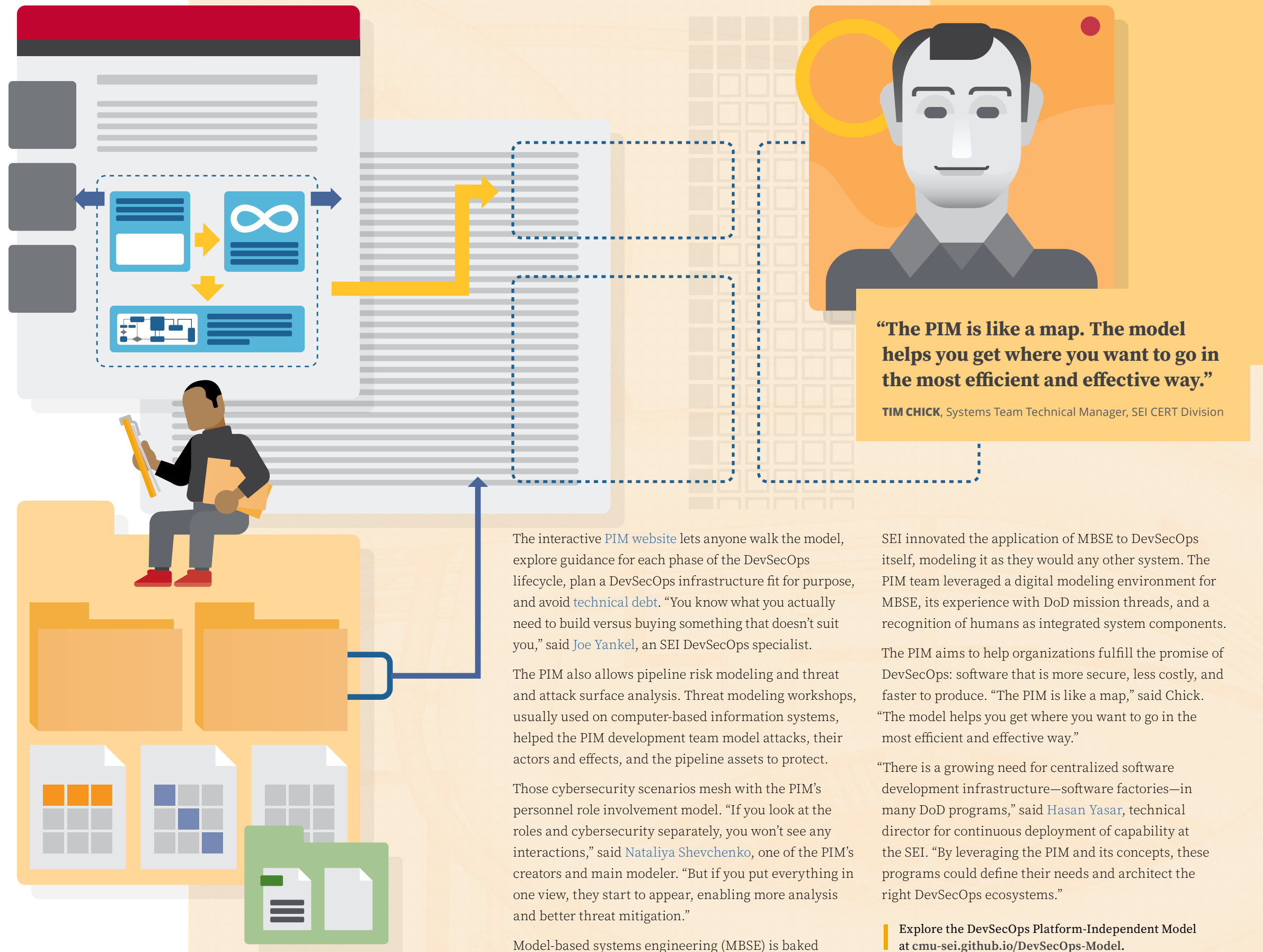
The SEI's [DevSecOps Platform-Independent Model \(PIM\)](#) formalizes the practices of DevSecOps pipelines and organizes relevant guidance. The first-of-its-kind, enterprise-wide model gives software development organizations a practical set of instructions for creating, maintaining, and evolving DevSecOps pipelines.

The DevSecOps software engineering environment promotes collaboration among development, security, and operations. This socio-technical system uses automation for flexible, rapid, frequent delivery of secure infrastructure and software to production.

Software development organizations must tailor each DevSecOps pipeline to the people, processes, and technology needed to provide a product or service. These complex pipelines are especially hard for large projects and those in [heavily regulated, security-sensitive environments](#).

“Programs often focus on the product and don’t put enough effort into the pipeline that’s building it,” said [Tim Chick](#), PIM project lead. Without practical guidance, organizations create pipelines ad hoc, fight fire after fire, and fail to get the expected value from their DevSecOps implementations.

The DevSecOps PIM is a reusable reference architecture for DevSecOps pipelines. It is a systematic, consistent starting point for new DevSecOps projects or a reference for assessing existing ones. Any stakeholder in software development—managers, executives, engineers, and acquisition officers—might find a use for the PIM’s holistic, enterprise-wide view.



“The PIM is like a map. The model helps you get where you want to go in the most efficient and effective way.”

TIM CHICK, Systems Team Technical Manager, SEI CERT Division

The interactive [PIM website](#) lets anyone walk the model, explore guidance for each phase of the DevSecOps lifecycle, plan a DevSecOps infrastructure fit for purpose, and avoid [technical debt](#). “You know what you actually need to build versus buying something that doesn’t suit you,” said [Joe Yankel](#), an SEI DevSecOps specialist.

The PIM also allows pipeline risk modeling and threat and attack surface analysis. Threat modeling workshops, usually used on computer-based information systems, helped the PIM development team model attacks, their actors and effects, and the pipeline assets to protect.

Those cybersecurity scenarios mesh with the PIM’s personnel role involvement model. “If you look at the roles and cybersecurity separately, you won’t see any interactions,” said [Nataliya Shevchenko](#), one of the PIM’s creators and main modeler. “But if you put everything in one view, they start to appear, enabling more analysis and better threat mitigation.”

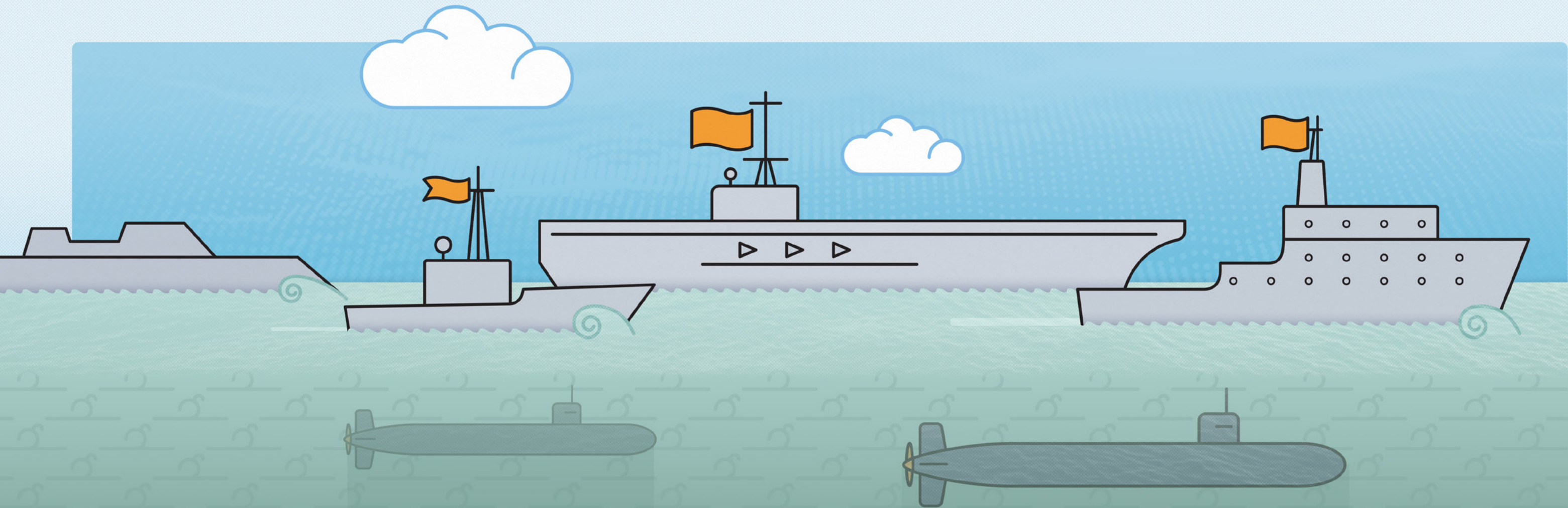
Model-based systems engineering (MBSE) is baked into the DevSecOps process. But to create the PIM, the

SEI innovated the application of MBSE to DevSecOps itself, modeling it as they would any other system. The PIM team leveraged a digital modeling environment for MBSE, its experience with DoD mission threads, and a recognition of humans as integrated system components.

The PIM aims to help organizations fulfill the promise of DevSecOps: software that is more secure, less costly, and faster to produce. “The PIM is like a map,” said Chick. “The model helps you get where you want to go in the most efficient and effective way.”

“There is a growing need for centralized software development infrastructure—software factories—in many DoD programs,” said [Hasan Yasar](#), technical director for continuous deployment of capability at the SEI. “By leveraging the PIM and its concepts, these programs could define their needs and architect the right DevSecOps ecosystems.”

Explore the [DevSecOps Platform-Independent Model](#) at [cmu-sei.github.io/DevSecOps-Model](#).



SEI Breadth and Depth Help DOT&E Adapt to Modern Software Development

Major Department of Defense (DoD) acquisition programs put their defense systems through rigorous operational testing and evaluation (OT&E). The Office of the Director, Operational Test and Evaluation (DOT&E) for the Office of the Secretary of Defense (OSD) oversees this process. OT&E of both hardware and software has traditionally occurred near the end of the system development lifecycle.

However, the [DoD Software Modernization Strategy](#) calls for the delivery of “resilient software capability at the speed of relevance.” To meet DoD mission goals, DOT&E is compressing its activities and shifting them earlier in the cycle. Since 2020, DOT&E has engaged the SEI for help meeting these challenges of modern software OT&E.

To deliver DoD software quickly in a rapidly changing threat environment, DOT&E is adopting a wide range of development approaches and new technologies. [Model-based systems engineering](#), [digital twins](#), [Agile](#), [DevSecOps](#), simulation, [artificial intelligence](#), [machine learning](#), and virtual reality all can play a part in rapid, iterative development. At the same time, they raise questions for testing and validation.

“Take, for example, integrating into an Agile workflow,” said [Nanette Brown](#), the SEI’s project lead on the DOT&E engagement. “The development team will do more validation with the customers of the specific capability being developed. But you must balance that with operational testing, which validates for the larger customer population.”

A team consisting of the SEI, other federally funded research and development centers, academic institutes, and DoD offices was assembled to assist DOT&E implement its strategy. The SEI helped develop policy and guidance documents for aligning software and cybersecurity T&E with modern software development practices such as Agile and DevSecOps. In particular, the SEI researched [acceptance test driven development \(ATDD\)](#) as a way to ensure that Agile processes capture OT&E requirements. This methodology will help DOT&E shift their activities to the left and reduce the likelihood of validation errors late in the lifecycle.

In 2022, the SEI began working with DOT&E to integrate its operational testing into the DevSecOps workflows of DoD systems development and acquisition programs. DOT&E is exploring the use of the SEI’s [DevSecOps Platform-Independent Model](#), which applies model-based systems engineering principles to DevSecOps pipelines, to guide this integration.

Another early-stage SEI effort is investigating the use of a continuous software bill of materials (SBOM). Using

open source software provides tremendous advantages to DoD acquisition programs: low cost, high reliability, and flexibility. However, the open nature of the software also increases its supply chain risk. The information contained in SBOMs will provide DOT&E the opportunity to manage and monitor supply chain risk and ensure the safety and integrity of open source software.

Testing and evaluating complex, software-driven national defense systems require breadth and depth of knowledge. The engagement with DOT&E exemplifies how the SEI weaves various teams and projects to address DoD challenges.

These branches of work share one goal for DOT&E: to test and evaluate defense systems with the quickness of DevSecOps and the reliability of traditional processes. Having oversight, accountability, and confidence in a rapid and iterative development environment will allow DOT&E to deliver software at the speed of relevance.

LEADERSHIP

CMU Leadership



Farnam Jahanian
President



James H. Garrett, Jr.
Provost and Chief Academic Officer



Theresa Mayer
Vice President for Research

SEI Executive Leadership



Paul Nielsen
Director and Chief Executive Officer



Anita Carleton
Director, Software Solutions Division



Heidi Magnelia
Chief Financial Officer



David Thompson
Deputy Director and Chief Operating Officer



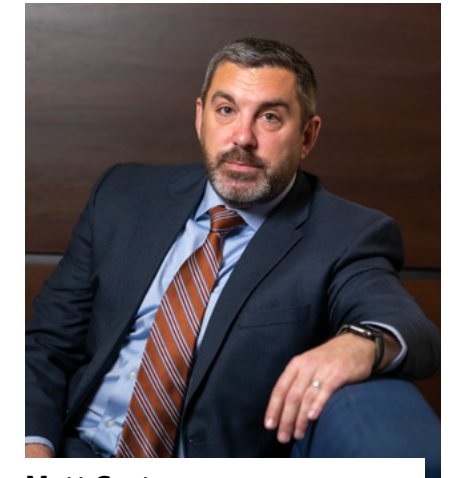
Gregory J. Touhill
Director, CERT Division



Mary Catherine Ward
Chief Strategy Officer



Tom Longstaff
Chief Technology Officer



Matt Gaston
Director, Artificial Intelligence Division



Sandra Noonan
General Counsel

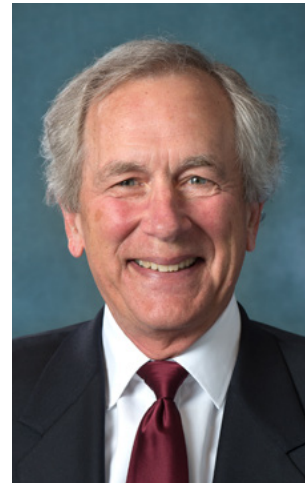
Board of Visitors

The SEI Board of Visitors advises the Carnegie Mellon University president, university provost, and SEI director on SEI plans and operations. The board monitors SEI activities, provides reports to the president and provost, and makes recommendations for improvement.



Russell Crockett

Managing Partner and CEO of Aeon Blue Technologies; Principal and Owner of RTC Energy LLC; Trustee, Carnegie Mellon University



Philip Dowd

Private investor; former Senior Vice President, SunGard Data Systems; Emeritus Trustee, Carnegie Mellon University



John M. Gilligan

President and CEO, Center for Internet Security (CIS); former President and COO, Schafer Corporation; former President, Gilligan Group; former Senior Vice President and Director, Defense Sector of SRA International; former CIO for the Department of Energy



Elizabeth A. Hight

Former Vice President of the Cybersecurity Solutions Group, Hewlett Packard Enterprise Services; former Rear Admiral, U.S. Navy; former Vice Director of the Defense Information Systems Agency



Tom Love

Chief Executive Officer, ShouldersCorp; Founder of Object Technology Group within IBM Consulting



Alan J. McLaughlin

Chair, Board of Visitors; Consultant; Former Assistant Director, MIT Lincoln Laboratory



Donald Stitzenberg

President, CBA Associates; Emeritus Trustee, Carnegie Mellon University; former Executive Director of Clinical Biostatistics at Merck; Member, New Jersey Bar Association

SEI Research Teams

Implementing the National Agenda for Software Engineering

Anita Carleton (project lead), Dionisio de Niz, Mark Klein

[p. 4](#)

SEI Co-Authored Papers Awarded by International Conferences

Grace Lewis, Robert Nord, Ipek Ozkaya, Edward Schwartz

[p. 4](#)

Juneberry Version 0.5 Simulates Attacks on Machine-Learning Systems

Andrew Mellinger (project lead), Bryan Brown, Matthew Churilla, Shannon Gallagher, Jon Helland, Daniel Justice, Dominique Mittermeier, Hayden Moore, William R. Nichols, William Shaw, Anusha Sinha, Nathan VanHoudnos, Jordan Widjaja, Nick Winski, John Zucca

[p. 5](#)

Implementing Responsible Artificial Intelligence

Carol Smith, Alex Van Deusen

[p. 6](#)

Modernizing Land-Based U.S. Nuclear Deterrent

Bob Stoddard (project lead), Carol Woody (project lead), Christopher Alberts, Björn Andersson, Luiz Antunes, Michael Bandor, Jeff Boleng, Dionisio de Niz, Robert Ellison, Michael Gagliardi, John Goodenough, Ted Marz, Christopher Miller, Suzanne Miller, William Nichols, Daniel Plakosh, Manuel Rosso-Llopert, Douglas Schmidt, David Shepard, Chuck Weinstock

[p. 7](#)

Zero Trust Industry Days Starts Critical Conversation

Tim Morrow (project lead), Trista Polaski, Kris Rush, Tara Sparacino, Greg Touhill

[p. 7](#)

Enabling Proactive Cyber Threat Detection in the Federal Civilian Executive Branch

Sean Hutchison (project lead), Katherine Prevost, Daniel Ruef

[p. 10](#)

AI Engineering Symposium Assembles AI Community

Rachel Dzombak (project lead), Matt Gaston

[p. 11](#)

Applying Causal Learning to Reduce Testing Times and Costs

Bob Stoddard (project lead), Nanette Brown, Mike Konrad, Melissa Ludwick, David Shepard, Nicholas Testa

[p. 13](#)

SEI Lends Expertise to Key Air Force Missile System Acquisition

David Walbeck (project lead), Stephen Beck

[p. 14](#)

Keeping Ahead of Insider Risk

Dan Costa (project lead), Carrie Gardner, Angela Horneman, Sarah Miller, Andrew Moore, Derrick Spooner, Michael Theis

[p. 16](#)

Codifying Test and Evaluation of Machine-Learning Aerial Object Detectors

Eric Heim (project lead), Tanisha Smith, John Zucca

[p. 18](#)

Increasing American Competitiveness in Semiconductor Chips

John Wohlbier (project lead), Andrew Dolgert

[p. 21](#)

Assuring Increasingly Autonomous Cyber-Physical Systems

Jerome Hugues (project lead), Aaron Greenhouse, Keaton Hanna, Sam Procter, Joe Seibel, Lutz Wrage

[p. 22](#)

Updated Energy Sector Cybersecurity Maturity Model Helps Keep the Lights On

Brian Benestelli (project lead), Patricia Flinn, Douglas Gardner, Jessica Hedges, Gavin Jurecko, Julia Mullaney, Alexander Petrilli, Jeffrey Pinckard

[p. 24](#)

New Model Provides Blueprint for DevSecOps

Tim Chick (project lead), Brent Frye, Lyndsi Hughes, Mary Popeck, Aaron Reffett, Nataliya Shevchenko, Carol Woody, Joe Yankel

[p. 26](#)

SEI Breadth and Depth Help DOT&E Adapt to Modern Software Development

Nanette Brown (project lead), Tim Chick, Brent Frye, Melissa Ludwick, Brigid Petrie O'Hearn, Forrest Shull, Brett Tucker, Joe Yankel, Charles Yarbrough

[p. 28](#)

Copyright

Copyright 2023 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM23-0260

Credits

Manager, Communication Services

Janet Rex

Manager, Public Relations

Richard Lynch

Manager, Communication Design

Cat Zaccardi

Editor-in-Chief

Paul Ruggiero

Editorial

Jenna Bodnar

Ed Desautels

Claire Dixon

Patricia Flinn

Lope Lopez

Tamara Marshall-Keim

John Morley

Sheela Nath

Sandy Shrum

Barbara White

Design

Christopher Baum

Illustration

Christopher Baum

David Biber

Kurt Hess

Todd Loizes

Digital Production

Mike Duda

SEI Pittsburgh, PA

4500 Fifth Avenue
Pittsburgh, PA 15213-2612

SEI Arlington, VA

4301 Wilson Boulevard
Suite 200
Arlington, VA 22203