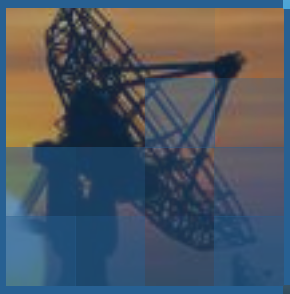
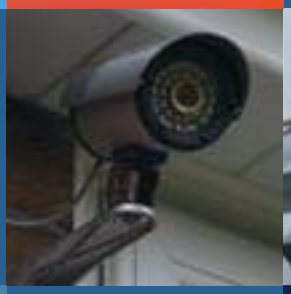
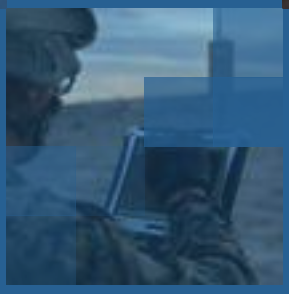
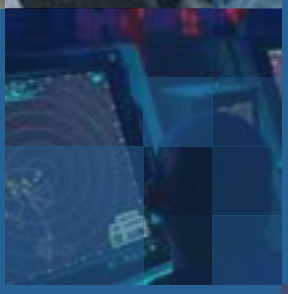
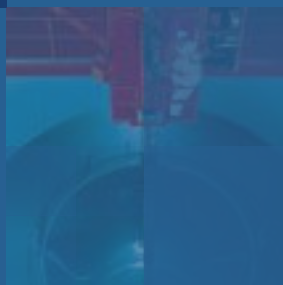
2015 YEAR IN REVIEW

Software Engineering Institute
Carnegie Mellon University®

The Software Engineering Institute (SEI) is a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

The SEI's mission is to advance the technologies and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring.

The *2015 SEI Year in Review* highlights the work of the Institute undertaken during the fiscal year spanning October 1, 2014 to September 30, 2015.

DIRECTOR'S MESSAGE

At the Carnegie Mellon University Software Engineering Institute (CMU SEI), our technical staff creates innovation from rigorous research and transitions technology to enhance our sponsors' capabilities and improve the state-of-the-practice in software and cybersecurity. In July 2015, the Department of Defense endorsed the enduring value of these efforts by renewing its contract with CMU for the SEI.

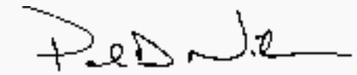
Our R&D work continues to meet current needs and form answers for tomorrow's challenges. In 2015, our engineers stepped in to help a prototyping team in a government lab accelerate its use of Agile methods in an acquisition for a critical U.S. Air Force intelligence system. At the same time, our researchers began building the foundations of new knowledge regarding how to increase people's trust in robots.

At the request of the Department of Homeland Security (DHS), we conducted an evaluation of risks associated with the emerging Internet of Things. In related work, we collaborated with the Department of Transportation and US-CERT on research aimed at securing the U.S. government's fleet of vehicles.

The SEI produces results by collaborating with government, academia, and industry. In 2015, we developed a Cyber Investigator Certification Program for the Federal Bureau of Investigation (FBI), conducted risk and vulnerability assessments for industry organizations, and collaborated with researchers from CMU and the Florida Institute of Technology on a dynamic network defense platform.

Over the last three years, we helped save the U.S. government about $70 million while training more than 125,000 cybersecurity workers using the SEI-developed Federal Virtual Training Environment (FedVTE).

Software drives the cyber environment on which everyone—our military, civil government, industry, and entire population—relies. Wherever you find software, you will find the SEI at work.

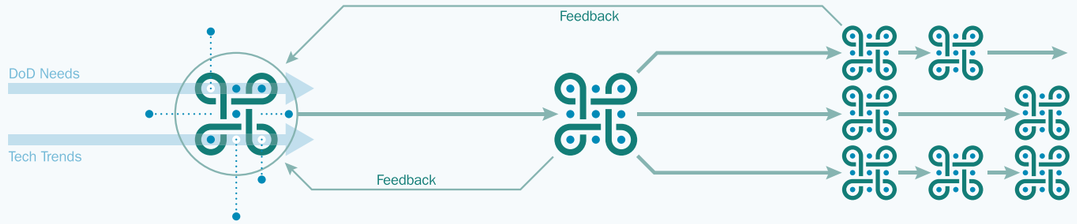


Paul D. Nielsen
Director and CEO

Table of Contents

STRATEGY

The SEI achieves its goals through technology innovation and transition. The SEI creates usable technologies, applies them to real problems, and amplifies their impact by accelerating broad adoption.



Create

The SEI addresses significant and pervasive software engineering problems by

- motivating research
- innovating new technologies
- creating prototypes and open-source software
- identifying and adding value to emerging or underused technologies
- improving and adapting existing solutions

SEI technologies and solutions are suitable for application and transition to the software engineering community and to organizations that commission, build, use, or evolve systems that are dependent on software. The SEI partners with innovators and researchers to implement these activities.

Apply

The SEI applies and validates new and improved technologies and solutions in real-world government and commercial contexts. Application and validation are required to prove effectiveness, applicability, and transition potential. Solutions and technologies are refined and extended as an intrinsic part of the application activities.

Government and commercial organizations directly benefit from these engagements. In addition, the experience gained by the SEI informs

- the "Create" activities about real-world problems and needed adjustments, technologies, and solutions
- the "Amplify" activities about needed transition artifacts and strategies

The SEI works with early adopters to implement the "Apply" activities.

Amplify

The SEI works through the software engineering community and organizations dependent on software to encourage and support the widespread adoption of new and improved technologies and solutions through

- advocacy
- web-based communication and dissemination
- books and publications
- certifications
- courses
- leadership in professional organizations
- licenses for use and delivery

The SEI accelerates the adoption and impact of software engineering improvements.

The SEI engages directly with the community and through its partners to amplify its work.

AREAS OF WORK

Software is critical to the system capabilities the Department of Defense (DoD) needs to achieve its mission. The pace of innovation in information technology (IT) is unmatched by any other technology crucial to the DoD's mission readiness and success. The expectations placed on software and IT have only increased. If the DoD is to acquire and deploy trustworthy software-enabled capabilities, it must address systems engineering, cybersecurity, and software engineering together from conception to sustainment.

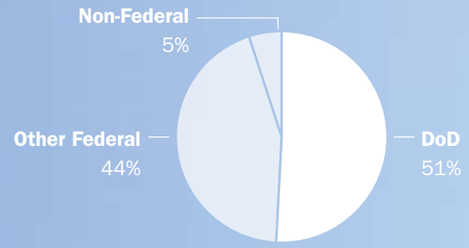
Since 1984, the Software Engineering Institute (SEI) has served the nation as a federally funded research and development center sponsored by the DoD. The SEI helps organizations improve their ability to acquire, develop, operate, and sustain software systems that are innovative, affordable, enduring, and trustworthy.

The SEI conducts research and development and publishes findings in these areas, and works together with partners and collaborators in industry, academia, and government. The SEI also undertakes pilot programs to refine best practices and inform its future technical direction. The SEI disseminates mature and proven solutions through software tools, training courses, licensing, and publication of best practices.

To support these objectives, the SEI focuses on several technical directions in the following major areas:

- **Software Engineering,** including issues of software system acquisition, design, development, integration, testing, sustainment, and measurement
- **Cybersecurity,** including activities related to the security of networks and computers, with a strong focus on deployable tools, methods, and workforce development
- **Assurance,** comprising a combination of techniques in software engineering and security that focus on a "designed-in" approach throughout the software lifecycle
- **DoD Critical Component Capabilities,** such as cyber-physical systems, high-performance computing and parallel algorithms, mobile applications, networking, and autonomous operations

Funding Sources



In FY 2015, the SEI received funding from a variety of sources in the Department of Defense, civil agencies, and industry.

IN THE NEWS

SEI Contract Renewed by Department of Defense for $1.73 Billion

In fiscal 2015, the U.S. Department of Defense (DoD) renewed its contract with Carnegie Mellon University for the Software Engineering Institute. The contract ensures that the Institute, a federally funded research and development center, will continue to support the nation's defense by advancing and transitioning the science, technologies, and practices needed to engineer and secure software systems.

The SEI, which is sponsored by the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, is the only FFRDC focusing specifically on software-related security and engineering issues. The contract was awarded for a term of five years with an option for an additional five years. The contract has an overall ceiling of $1.73 billion.

"It is an honor for CMU to be selected to manage the government's research and development center for software engineering and cybersecurity at such a critical time for this work," university President Subra Suresh said. "CMU's expertise in securing systems and combatting cyberattacks is a university-wide strength across the SEI and various academic units, and this work is becoming increasingly important not only for national defense but also for individual citizens, critical infrastructure, and commercial enterprises."

"The collaboration between CMU and the SEI provides tremendous benefits to both the university and the institute, making possible accomplishments neither could realize on its own," said CMU Provost Farnam Jahanian. "Together, CMU and the SEI will support the missions of our nation's defense and civilian agencies and collaborate with industry partners to advance and transition innovative technologies."

Complex software systems requiring the highest levels of cybersecurity now underpin the operations of the DoD, the Department of Homeland Security, and other government agencies and industries in our software-dependent society. As part of Carnegie Mellon University, one of the world's leading academic institutions for research and education in computer science and engineering, the SEI is uniquely positioned to develop technologies and practices through its own research and to apply innovative technologies developed by outside organizations to solve difficult engineering and cybersecurity challenges in various fields, including aerospace, transportation, banking and finance, energy, robotics, and industrial automation.

"The renewal of our contract is a strong endorsement of the value the SEI's women and men provide at a time when cybersecurity and software quality are critical to our national security," said Paul Nielsen, SEI director and CEO. "Our new contract guarantees that the SEI can continue to develop breakthrough technologies in collaboration with Carnegie Mellon University, the Department of Defense, and our industry partners. It also ensures that hundreds of excellent technology jobs remain in Pittsburgh for the foreseeable future, and that the SEI will continue to be a high-tech anchor for the region."

Greg Shannon
SEI CERT Division
Chief Scientist

Greg Shannon Joins White House Office of Science and Technology Policy

In July 2015, Dr. Greg Shannon, chief scientist for the SEI CERT Division, joined the White House Office of Science and Technology Policy (OSTP) as assistant director for cybersecurity strategy in the National Security and International Affairs Division.

IEEE-USA provided a fellowship to Carnegie Mellon University to partially support faculty or staff who have the opportunity to serve temporarily in the Executive Office of the President.

As chief scientist, Shannon led the SEI's CERT Division to advance the science of cybersecurity with new research capabilities for the Defense Advanced Research Projects Agency, the Intelligence Advanced Research Projects Agency, and the Department of Homeland Security.

In his role at the OSTP, Shannon works on

- innovation and policy in cybersecurity research and development
- effective and efficient cybersecurity technologies and practices
- the interdependence of security and privacy
- sustainable diversity of thought in the cybersecurity workforce

OSTP is authorized by Congress to "lead interagency efforts to develop and implement sound science and technology policies and budgets, and to work with the private sector, state and local governments, the science and higher education communities, and other nations toward this end."

Shannon recently served as general chair for the IEEE Symposium on Security & Privacy and was chair of the IEEE Cybersecurity Initiative until August.

"My goal as chair was to accelerate innovative research, development, and use of efficient cybersecurity and privacy technologies that protect commerce, innovation, and expression," Shannon said.

Harry
Levinson

Helping Air Force Intelligence Adapt to Agile Methodology

The Software Engineering Institute is helping the U.S. Air Force transition one of its most important—and complex—weapon systems to respond quickly and efficiently to new intelligence data sensors, formats, and analysis. Throughout 2015, an SEI team advised the Air Force program office for the Air Force Distributed Common Ground System (AF DCGS) as it prepared to start acquiring systems work performed in accordance with Agile development principles.

"We're supporting the Air Force Research Lab prototyping team's effort to enable Agile software development by teaching them how to execute and transition Agile methodology and adapt it to Air Force acquisition processes," said Harry Levinson, the project lead at the SEI. "This is a major project for a major Air Force system asset."

The Air Force describes AF DCGS as its primary weapon system for intelligence, surveillance, reconnaissance, planning, direction, collection, processing, exploitation, analysis, and dissemination. It employs a global communications architecture that connects multiple intelligence platforms and sensors. It currently comprises 27 regionally aligned, globally networked sites.

Although U.S. involvement in military operations in Afghanistan and elsewhere in the world has wound down substantially over the past few years, the need for AF DCGS has not. "If anything," Levinson noted, "the AF DCGS is becoming more important and more valuable."

Indeed, operating the system at the high level of performance needed in the current military environment requires a near constant stream of upgrades, updates, and additions to the AF DCGS computer systems—particularly the software. Anticipating that much of this software development will be done using Agile development methods, the Air Force asked the SEI to help its acquisition teams become skilled in applying Agile approaches to the key task of specifying and defining requirements for software.

The project is led by AF DCGS Program Manager Lt. Col. Joshua Williams. And, while the Air Force Research Lab's contingent for the work is located in Rome, New York, the team has also been educating and training personnel at Robins Air Force Base in Georgia, Hanscom Air Force Base in Massachusetts, and Langley Air Force Base in Virginia.

The project was launched in October 2014 and continued at a steady pace through 2015. A team of about a dozen SEI experts conducted various training and coaching events during 2015 at various locations, providing everything from formal classroom training to learn-on-the-go brown bag lunch events and in-execution mentoring.

Additional training and program activities are expected to continue in 2016.

"Adopting Agile has not been easy," Williams said recently. "It has brought significant change to our acquisition and development strategies and practices. But overall, it's helped AF DCGS be more efficient, effective, and affordable."

For more information on the SEI's work on Agile in the Department of Defense, visit.sei.cmu.edu/acquisition/research/.

"We're supporting the Air Force Research Lab prototyping team's effort to enable Agile software development by teaching them how to execute and transition Agile methodology and adapt it to Air Force acquisition processes."

—Harry Levinson, SEI Project Lead

Photos: U.S. Air Force

Art Manion

Tackling Security Risks in Internet-of-Things Devices

Devices that connect to the Internet, such as cars, insulin pumps, baby monitors, and even household appliances like coffee makers, are growing in number and complexity—and therefore in risk. Most of them weren't built with security in mind, leaving them vulnerable to attacks by malicious outsiders.

To help reduce that risk and help Internet-of-Things (IoT) vendors make these devices more secure, the U.S. Department of Homeland Security (DHS) asked the SEI to examine them, evaluate their risks, and prioritize those IoT domains with the most critical need for security measures and protections. The SEI identified several safety-related sectors: vehicle autonomy (self-driving vehicles); smart medical devices, such as pacemakers and insulin pumps; airplanes; and smart sensors, such as home security systems. Another sector of concern is low-priced ubiquitous devices, such as baby monitors, video cameras, and home Internet routers.

The SEI published its recommendations for devices in several of these domains in the 2015 technical report *Emerging Technology Domains Risk Survey*. In addition to that report, SEI researchers are getting the word out by talking to industry groups such as the Alliance of Automobile Manufacturers and the Medical Device Vulnerability and Information Sharing Initiative (MD-VISI). The SEI advocates threat modeling that accounts for these new risks and coordinated vulnerability disclosure that minimizes costs associated with fixing vulnerabilities.

"DHS needs a way to phase its approach to addressing risks and vulnerabilities in the rapidly expanding IoT marketplace," said Tom Millar, Chief of Communications at the U.S. Computer Emergency Readiness Team (US-CERT). "The SEI's CERT research and recommendations help tremendously in informing our decisions and keeping us well positioned to deal with threats as they arise."

Because of safety concerns, many of the critical IoT domains are regulated, such as vehicle autonomy and smart medical devices. For that reason, the SEI is talking to regulators about where security can be improved and, when possible, how to work security into existing regulations rather than develop new ones.

Art Manion, a senior vulnerability analyst at the SEI's CERT Coordination Center, describes the challenge this way: "IoT vendors should be able to receive vulnerability reports, make any needed fixes, and deploy fixes or mitigations in a reasonable time frame. Vendors should also update their threat models to account for the exposure to intelligent adversaries that comes with connectivity. These two strategies are key starting points for IoT security, particularly in safety sectors. We're only going to see more 'things,' so we need to find ways to support vendors as they prepare for and respond to security threats in these products."

"We're taking all of these new technologies that are being developed independently and bringing them together. We're finding where they might conflict and where they might complement one another, and ultimately making them usable for our government customers."

—Andrew Mellinger, SEI Emerging Technology Center

Andrew Mellinger

Be Unpredictable: Dynamic Network Defense Improves Security

A moving target is more difficult to hit than one that's standing still. This concept is foundational to dynamic network defense, an approach to network security that hinges on creating unpredictable conditions for cyber attackers. This area of research is advancing rapidly, and with that growth comes the need for an approach that considers how newly developed techniques can work together.

In October 2015, staff members from the SEI's Emerging Technology Center began a multi-year project to respond to this need by creating a reference implementation for a dynamic network defense platform—a standard by which future implementations and customizations can be evaluated.

"We're taking all of these new technologies that are being developed independently and bringing them together," said the project's principal investigator, Andrew Mellinger. "We're finding where they might conflict and where they might complement one another, and ultimately making them usable for our government customers."

The project has three overarching goals: adoptability, security, and extensibility. "We have to make sure our platform is usable for the people who need it, that it's designed securely from the ground up, and that it can be customized and added to," Mellinger explained. To achieve those goals, the team is working toward a number of specific objectives for the platform.

The SEI's solution will accommodate and balance a variety of techniques from any layer of the "stack"—from policy to operating system to network and beyond. Examples include requiring periodic password changes to create a changing environment, IP hopping to make networks difficult for attackers to probe, and redundant data to allow for double-checks and restoration. And by working in a decentralized fashion—spreading services across a network so that services continue to be available even if one part of the network is disabled—the SEI platform will minimize the danger of single points of failure.

The platform will have a rich data model for advanced planning, meaning it will take advantage of analytics as well as proactive operations (routine actions thought to protect a network) and predictive operations (actions based on actual information collected from sensors and other sources).

Human users factor prominently in the development of the platform: rather than simply performing complex and sometimes confusing operations on its own, the platform will provide strong human-in-the-loop support to ensure that users have a role in decision making and that the platform is transparent to the user defending the network. Not least is the ability of the platform to be extended and customized by its users.

The project will run through 2017. The team is currently building the reference platform and has created a walking skeleton, which Agile co-founder Alistair Cockburn has referred to as "a tiny implementation of the system that performs a small end-to-end function." The SEI team is collaborating with researchers from the Florida Institute of Technology and Carnegie Mellon University and is taking advantage of Carnegie Mellon's tremendous body of work in self-adaptive systems.

"We're considering the advances being made in research and how they can be applied to our customers' needs," said Mellinger. "This kind of work is really at the sweet spot of the SEI's mission."

Peter Feiler

Julien Delange

Extending the Reach of Architecture Analysis & Design Language

The strategy of the SEI is to *create* usable technologies, *apply* them to real problems, and *amplify* the impact. The SEI has made significant advances in all three areas this year in its work with the Architecture Analysis & Design Language (AADL). SAE International released AADL as a standard in 2004 to address a common problem in development: mismatched assumptions about the physical system, computer hardware, software, and their interactions could result in system problems detected too late in the development lifecycle. This creates an increasingly unaffordable and potentially dangerous situation for developers and users of mission- and safety-critical technologies.

"A key to improving this situation is for developers to perform virtual system integration with the AADL model throughout the development lifecycle and discover system-level issues closer to the time they are introduced," said Peter Feiler, a principal research scientist at the SEI who was instrumental in the development of AADL.

Create

Since its initial release, the SAE AS-2C committee on AADL under Chair Bruce Lewis, a senior researcher from the U.S. Army Aviation & Missile Research Development & Engineering Center, and Feiler, the SEI technical lead, has played an active role in the "create" phase of this technology by revising the AADL core standard and extending it into a standard suite. This year, the committee released three new annexes.

SEI researcher Julien Delange authored the Avionics Application Standard Software Interface (ARINC653) Annex, which supports verification and auto-generation of configurations for partitioned avionics systems. The Error Model Annex (EMV2), revised by Feiler since its original release in 2006, includes a fault effects taxonomy and supports automation of the system safety assessment process and extends it into the software system architecture.

The Code Generation Annex, authored by Jerome Hugues from the Institut Supérieur de l'Aéronautique et de l'Espace (ISAE) in France, defines a mapping between AADL components and implementations in C and Ada.

Apply

This was a year of growth for AADL in the SEI's "Apply" phase as new organizations chose to use it in their work. In the DARPA High-Assurance Cyber Military Systems program, the Secure Mathematically-Assured Composition of Control Models project chose to use AADL in its work to reduce security risks of software in unmanned vehicles. A red team was unable to penetrate their software over a six-week period, despite access to source code, thanks to contract-based compositional verification, auto-code generation from verified models, and a certified real-time OS kernel. The U.S. Army Joint Multi-Role Technology Demonstrator (JMR TD), which is helping to develop the DoD's next-generation rotorcraft fleet (Future Vertical Lift), is accelerating its adoption of AADL after a successful shadow project by the SEI and Adventium Labs in 2014 showed potential requirements and system-integration issues could be identified early in the development process.

Amplify

To make it easier to use AADL and amplify its reach, a number of tools have been developed by the SEI and other organizations. The SEI led the development of the Open Source AADL Toolset Environment (OSATE) workbench, which has become a prototyping and transition vehicle for a number of teams in architecture-centric research projects around the world. This year, a number of updates were made to the toolset, including enhancements to the graphical editor and several analysis capabilities, and the creation of a workflow layer that will extend its adoption by practitioners.

For more information on the SEI's work in AADL, visit sei.cmu.edu/architecture/tools/analyze/.

Photo: U.S. Army

Neil Ernst

Survey Offers Keys to Understanding and Managing Technical Debt

Software development involves compromises between speed and quality. Technical debt weighs the trade-offs between taking shortcuts to quickly deliver features and applying sound software engineering principles to produce high-quality code. The SEI's Architecture Practices team investigates how organizations conceptualize and handle technical debt.

In 2015, the team surveyed more than 1,800 software engineers and architects to discover how they handled technical debt on large, long-term projects. Key findings include the following:

- Poor architecture choices are the most frequent source of technical debt and the most difficult to fix. Monitoring and tracking design drift is vital.
- Software tools do not capture the full extent of technical debt, especially for architectural debt. Issue tracking and social processes were the most popular ways to manage it.
- Developers have few formal practices for handling technical debt.

Software projects incur technical debt when they prioritize immediate business needs over the system's design, infrastructure, and architecture. This isn't necessarily a bad thing—for example, a customer's urgent request may be important enough to justify an intermediate solution. But this debt must be monitored and eventually paid off by reworking the software. Well-managed technical debt helps developers rapidly add capabilities while preserving maintainability and extensibility. Badly managed technical debt leads to poorly designed software with low code quality; eventually it becomes a barely maintainable mess.

"Technical debt is context-dependent," said SEI researcher Neil Ernst. "If you are working on a smaller project, or a younger project perhaps, these issues are not as relevant. The projects that had the biggest problems were 10 to 15 years old. They had up to millions of lines of code."

The Architecture Practices team also launched a one-day introductory course, "Managing Technical Debt in Software." In addition, it worked with organizations in industry and government to establish sound practices for managing technical debt, including prioritizing its most significant contributors, introducing technical debt into backlog management practices, and piloting code quality measurements.

The Architectural Practices team's ongoing research focuses on tools that pinpoint key sources of technical debt in software systems. The team's goal is to provide data-driven, empirically validated results that identify the largest contributors to technical debt that would benefit from tool support.

For more information on the technical debt survey and its results, visit insights.sei.cmu.edu/sei_blog/2015/07/a-field-study-of-technical-debt.html.

Kris Rush

SEI Develops Cyber Investigator Certification Program for FBI

With serious cybercrime on the rise, the FBI recognized the need for more law enforcement professionals, at all levels, equipped to handle crime scenes involving computers and digital artifacts. In particular, law enforcement first responders need to know how to survey and secure these crime scenes without compromising the integrity of evidence. To help meet this need, the FBI conceived a Cyber Investigator Certification Program, and it enlisted the help of the SEI to develop it.

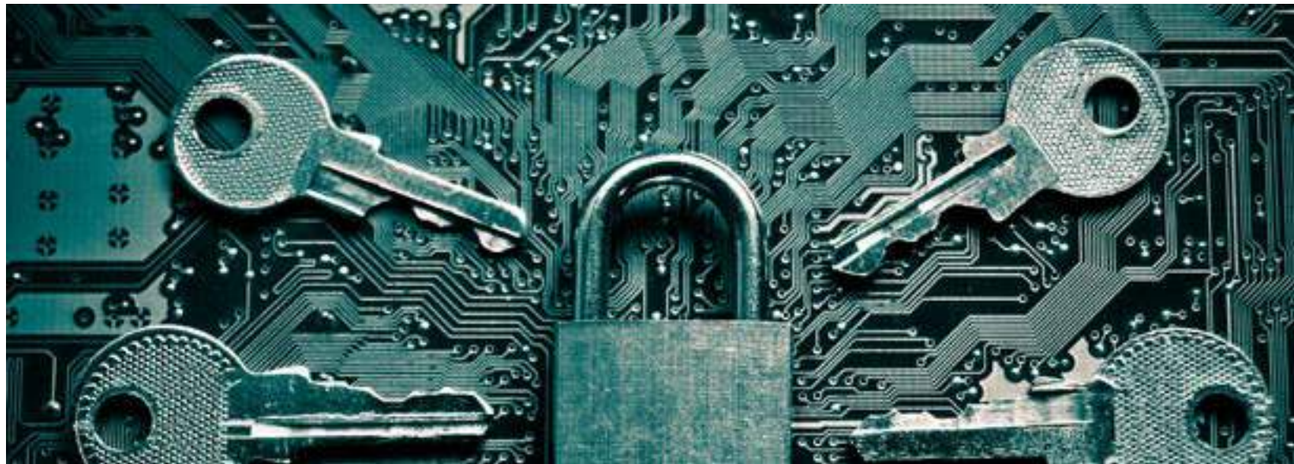
Working with the FBI's Cyber Division and the International Association of Chiefs of Police, experts at the SEI developed a self-guided online program designed to improve a first responder's technical knowledge, in particular the investigative methodology specific to cyber investigations.

"In developing this program, we were able to draw on the talent and resources of Pittsburgh's growing film industry to create engaging, realistic scenarios," said the SEI's Kris Rush, technical director of the SEI CERT Division's Monitoring and Response Directorate. "We also leveraged the capabilities of the CERT STEPfwd training environment to deliver the course," added Rush. STEPfwd (Simulation, Training, and Exercise Platform) makes available from a web browser components from traditional classroom training, including lectures, slide presentations, hands-on labs, team cyber exercises, and quizzes. STEPfwd is a flexible, multimedia, e-learning environment that students can access anywhere, anytime.

To earn a certificate, participants must complete the course and pass the assessment administered at the conclusion of the program. The course is open to all federal, state, local, tribal, and territorial first responders with an account on the FBI's Law Enforcement Enterprise Portal.

Law enforcement personnel interested in this training can visit https://www.cjis.gov/onlineapp.

For more information on STEPfwd, visit cert.org/cyber-workforce-development/solutions.cfm.



Jim McCurley

Understanding Software Costs in the Department of Defense

Software has far eclipsed hardware in providing functionality in Department of Defense (DoD) systems: 90 percent of a weapon system's functionality can depend on software. This makes managing software throughout its lifecycle critical to controlling the performance and costs of DoD programs. Yet, actionable data to guide this task can be hard to come by. The aim of the SEI's Empirical Research Office (ERO) is to change that. As part of its efforts, the ERO is publishing software factbooks based on analyses of software engineering data to provide insight into policy and management questions about DoD software projects.

The impetus for this work was the challenge in determining how much the DoD actually spends on software.

"We wanted to take data that the DoD was already collecting, in the form of Software Resources Data Reports, and answer questions that really make a difference to those charged with funding and managing software-intensive projects," said Jim McCurley, an SEI researcher. Among the questions the ERO has investigated are, "What differences are there between best-in-class and worst-in-class software projects in the DoD?" and "How much does it cost to develop different types of software systems?" One surprising finding from this line of questioning is that real-time software is approximately four times the cost of automated information system software.

The results of this work are helping the sponsor get the most value out of all of its data.

To review the *DoD Software Factbook*, visit resources.sei.cmu.edu/library/asset-view.cfm?assetid=453262.

Photo: U.S. Army

Matt Gaston

The Future Is Now: SEI Emerging Technology Center Equips Government to Reap Benefits of New Technology

Whiteboards filled with mathematical equations, ideas for data visualizations, sticky notes from human-centered design activities, and notes from a cyber intelligence exercise greet visitors to a second-floor space in Carnegie Mellon's Collaborative Innovation Center. A small robot charges up in the corner near the conference room. Teams work together in group offices around a common area where a poster-sized red octagon commands—both playfully and seriously—"STOP. Collaborate and listen." The feeling is startup-meets-university, and the work focuses on the practical needs of real government customers.

The Emerging Technology Center (ETC) is the SEI's newest technical program, joining the Software Solutions Division and CERT Division in 2013. Its mission is to look to the future to prepare government organizations to take full advantage of the technologies that are changing our world.

"We're looking at 'recently possible' technologies that range from 3D printing to autonomy to the ability to quickly process huge amounts of data and making those things practical," said ETC Director Matt Gaston.

The ETC has come a long way from its humble beginnings as a "small but mighty" handful of staffers with a mandate to help the government leverage innovation.

This year, technical experts delivered a predictive analytics course developed for a government customer, provided thought leadership in cyber intelligence in support of the interagency Special Cyber Operations Research and Engineering (SCORE) Working Group, continued building a software library for complex graph analytics, conducted learning events for members of the ETC's Cyber Intelligence Research Consortium, and worked with government customers on several ongoing projects.

Also in 2015, ETC technical experts proposed several new projects that will stretch into 2016 and 2017. One of these, an effort to extract biometric data from video, could provide a flexible approach to airport security, evaluating post-traumatic stress disorder in returning soldiers, and detecting spoofed (for instance, photographic) faces to bolster current identification techniques.

ETC experts are also working to enhance the way robots explain their actions to ultimately increase users' trust. This work fills a critical need as the DoD relies increasingly on autonomy, and users must understand robot behaviors to allow them to perform dangerous jobs like search and rescue or explosives detection.

A project to establish benchmarks for selecting scalable machine learning platforms promises to create a level playing field that will help government and industry organizations choose the right tools for data-driven decision making.

Another ETC project seeks to bring modularity to additive manufacturing, an approach that applies foundational concepts of software engineering to 3D printing to increase the speed and flexibility of producing custom objects.

"New technologies make amazing things possible, and every day we help bring those amazing possibilities to bear on real mission needs," said Gaston.

To learn more about the work of the ETC, visit sei.cmu.edu/about/organization/etc.

"It's exciting to see our tools evolve to meet that analysis need by recording as much information as possible when encrypted communications are established."

— Sid Faber, SEI Situational Awareness team

Photo: U.S. Navy

Sid Faber

SEI Tools Promote Situational Awareness

Service to government and community has long driven the work of the SEI CERT Division's Situational Awareness (SA) team, as it did in 2015. For starters, the SA team released a number of new tool capabilities for analysts in the computer network defense community. To support their efforts in network traffic analysis and incident response, the SA team matured its suite of traffic collection and analysis tools called System for Internet Level Knowledge, or SiLK. These tools are specifically designed to enable security analysis on large networks.

SiLK's Analysis Pipeline capability is particularly important to analysts. It reads streaming network flow data from the traffic collection system. When combined with the sensing tool Yet Another Flowmeter (YAF), which is also part of the SiLK network tool suite, Pipeline can search traditional network flow data (IP addresses, ports, and protocols) in near real time. This new capability allows Pipeline to search for domain names and SSL certificates in traffic and immediately pass alerts when they match a potential threat. Sid Faber, senior network analyst on the SA team, explained the enhancement: "Pipeline moves the tool site from a retrospective analysis workflow into a near-real-time alerting workflow. Previously, the analysis pipeline only processed traditional, fixed-format network flow records. In 2015, the capability was improved so that Pipeline can now create metrics and alerts on the more flexible IP Formatted Exchange (IPFIX) data format, enabling it to essentially process nearly any type of data record."

CERT researchers also addressed the ever-increasing challenge encryption poses to network monitoring. It did so by enhancing YAF to capture details about certificates and other traffic features necessary to establish encrypted communications. "In general, we see the continued migration to end-to-end encrypted communications, which creates a real challenge for network-based monitoring," said Faber. "We've also seen the community respond by creating new analysis methods that study how that encrypted communication is established. It's exciting to see our tools evolve to meet that analysis need by recording as much information as possible when encrypted communications are established."

The CERT Division has also used reference implementations of security solutions to aid in acquisition support. "We recognize the challenge of deploying commercial security tools to address the unique needs of government, as well as the necessarily long acquisition cycle for deploying new cyber technology," said Faber. "We're addressing government needs by operating a data center designed specifically for vendors to demonstrate capability in an environment similar to the government's network. With sophisticated traffic generation techniques and supporting simulated infrastructure, we do more than just try out a new tool. We optimize a proposed architecture for wide-scale deployment, and if the government chooses to adopt the solution, we transition knowledge gained from the evaluation to streamline acquisition and deployment."

For more information about situational awareness tools created by the SEI's CERT Division, visit cert.org/netsa/tools/.

Mary Ann Lapham

Robert Nord

Ipek Ozkaya

Hasan Yasar

SEI Facilitates Adoption of Agile in Government Settings

In 2015, the SEI intensified its effort to explore and facilitate the adoption of Agile software development principles. As in past years, the institute emphasized sharing its expertise and know-how with both Department of Defense (DoD) and civilian government organizations. Key among the SEI's efforts in this area is its research on Agile in government settings.

Launched in 2009, the Agile Adoption in Government Settings project helps acquisition professionals in the DoD and other federal agencies interact effectively with contractors who use Agile methods. The biggest hurdles facing these organizations include new terminology, unfamiliar processes and procedures, and the need for a collaborative acquisition culture. Agile methods are characterized by close collaboration between customers and developers, frequent incremental deliveries of software, and evolution of requirements and designs as more is learned about the system and its intended use.

As of the end of 2015, the SEI had assisted ten U.S. Air Force programs with Agile coaching, training, advice, metrics, and test support. Three U.S. Army programs engaged the SEI for Agile training and support, and two U.S. Navy programs sought SEI help with Agile projects. An additional five civilian agency programs benefitted from SEI Agile expertise, along with several intelligence organizations.

"Our investment in exploring how to use Agile in government settings is paying valuable dividends across the government development space," noted Mary Ann Lapham, who heads this SEI research effort. "Agile is gaining adherents and proponents at a much faster rate than when we started the program."

The SEI also expanded other Agile-related activities in 2015: Lapham's team produced a comprehensive series of podcasts on the major principles of Agile, published additional entries in the SEI Blog on Agile concepts and their application in real-world scenarios, and published an additional entry in the Agile technical note series—*Contracting for Agile Software Development in the Department of Defense: An Introduction*.

By leveraging its ongoing relationships with DoD acquisition, as well as its experience with civilian government agencies, the SEI has developed a wealth of resources to help the DoD make informed decisions about the use of Agile in achieving its goals for speed, adaptability, and efficiency.

For more information, visit sei.cmu.edu/acquisition/research/.

More SEI Agile Research and DevOps Development

Agile principles were at the center of multiple SEI research and development programs:

- The Software Architecture team, led by Robert Nord and Ipek Ozkaya, continued its work with industry and government organizations adopting Agile development methods, helping them introduce software architecture practices into their lifecycle, with a particular focus on quality attributes.
- In the SEI's CERT Division, a team led by Hasan Yasar focused on **DevOps**. Yasar explained that DevOps is the extension of Agile principles to the development and operations (Dev+Ops) of software and systems. "DevOps implements Agile methodologies to the next level by focusing on tight collaboration between software developers and other technical experts (such as IT operations and security staff)," he said, "as well as substantial automation throughout the development lifecycle, and design and/or refactoring of systems to enable maximal agility in deployment and sustainment." The team provides guidance to organizations starting DevOps programs, and—like the architecture team—is working to add quality attributes to DevOps processes, especially security and compliance.

Photo: U.S. Navy

Participants in the Cyber Intelligence Research Consortium crisis simulation exercise were charged with a modest task: Save the world by finding the source of a dire biological terror threat and developing a threat assessment to put it into context for decision makers.

Jay McAllister

Rotem D. Guttman

Melissa Ludwick

Crisis Simulation Helps Cyber Intelligence Research Consortium Members Hone Skills

In July 2015, SEI Cyber Intelligence Research Consortium members gathered in Pittsburgh for the organization's first crisis simulation exercise. The two-day event, hosted by the SEI's Emerging Technology Center (ETC), brought together participants from member organizations in the government, military, and industry sectors, including PNC and American Express. The participants were charged with no small task: Save the world by finding the source of a dire biological terror threat and developing a threat assessment to put it into context for decision makers.

In kicking off the exercise, SEI Director and CEO Paul Nielsen said, "The military conducts a lot of exercises like this. They help you identify gaps and policy or operational issues you might have." Nielsen noted that the Cyber Intelligence Research Consortium is trying to bridge the gap between industry and government. "We want this to be the first of a series of such events involving members of the consortium."

To bring this scenario to life, SEI experts enriched the exercise using video, live action, fictional websites, and a fully functional simulated Internet environment provided by the SEI CERT Division's STEPfwd platform. Participants with an intelligence background focused on identifying the malicious actors and determining the relationships between events, while those with a technical background focused on reverse engineering a tool produced by the terrorist organization and reviewing evidence collected by field agents based on their findings. Two participants functioned as liaisons between the two groups and coordinated their efforts.

Groups from across the SEI collaborated to produce the simulation. The SEI CERT Division's Cyber Workforce Development team created large, simulated networks for participants to explore and authored custom malware for use by the threat actors. The SEI's Emerging Technology Center created a trove of intelligence artifacts for participants to analyze. The CERT Division's Network Situational Awareness team contributed a flow data analysis component. In addition, the SEI's Asset Creation, Collection, and Conversion team facilitated the creation of a series of high-quality briefing videos to immerse the participants in their role as agents.

"The event was a great success," said the SEI's Jay McAllister, ETC senior analyst and technical lead of the Cyber Intelligence Research Consortium. "It's a testament to what the SEI can accomplish when folks with different backgrounds and department identifiers come together to build something that showcases the awesome power of the SEI at large."

To learn more about the Cyber Intelligence Research Consortium, visit sei.cmu.edu/about/organization/etc/overview.cfm

STEPfwd is a virtual training environment that offers a rich library of cybersecurity and information assurance training. To learn more about STEPfwd, visit https://stepfwd.cert.org.

Scott McMillan

Eric Werner

Emerging Technology Center Tackles Intelligence Analysis in New Big-Data Environments

The past year saw continued research and development in the area of graph algorithms, which are widely used in analytical contexts in Department of Defense (DoD) applications. Graphs are used to represent many kinds of complex point-to-point relationships in the physical, cyber, and other realms and which span a number of operational areas, including intelligence analysis, autonomous systems, cyber intelligence and security, and logistics optimization. Graph analytics applications in these environments must execute at increasingly larger scales and increasingly higher rates to accommodate the growing velocity, volume, and variety of data sources.

Implementations of graph algorithms to achieve the highest levels of performance are complex and intimately tied to the underlying architecture. New and emerging computing architectures require new and different implementations of well-known graph algorithms, yet it is increasingly expensive and difficult for developers to implement them in ways that fully leverage their capabilities.

To address this challenge, researchers from the SEI's Emerging Technology Center (ETC) have for several years been investigating approaches that will make high-performance graph analytics on new and emerging architectures more accessible to users. This project, led by principal investigator Scott McMillan, involves researching the best practices, patterns, and abstractions to enable the development of a software graph library that separates the concerns of expressing graph algorithms from the details of the underlying computing architectures.

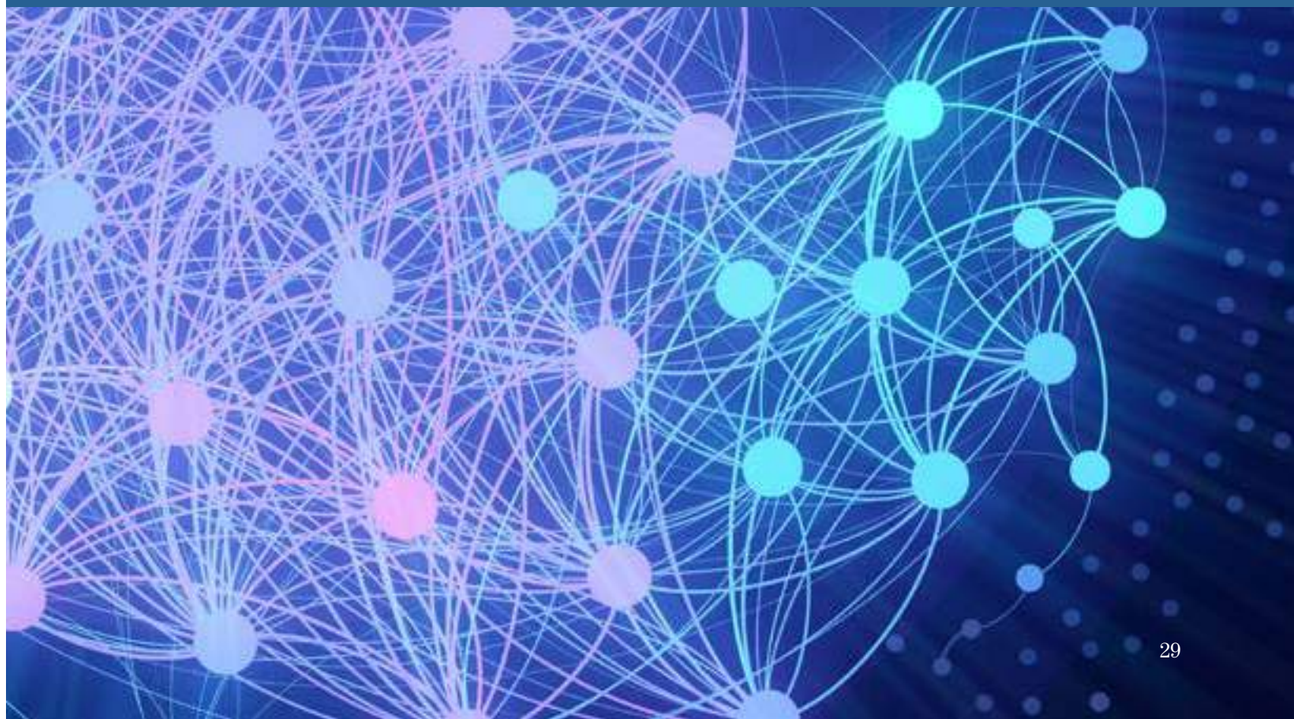
In 2015, the ETC turned its attention to researching algorithms that would facilitate graph analysis in ever-more-complex high-performance computing architectures. "We want to separate the concerns between the graph expertise needed to develop advanced graph analytics and the hardware expertise needed to achieve high levels of performance on these emerging architectures," said McMillan. "We've joined with other leading experts from industry, academia, and government to create an application programming interface standard called Graph Basic Linear Algebra Subprograms (GraphBLAS) meant to codify this separation of concerns."

The SEI's recent work on the GraphBLAS API is helping to spur a number of advancements. For instance, a growing library of graph algorithms developed as part of this project means algorithms can be implemented with less code. Furthermore, development of a specification for the GraphBLAS API will net improved standardization. In addition, the SEI's collaboration with Andrew Lumsdaine of the Center for Research in Exascale Technologies has resulted in more effective algorithm tuning for implementations in graphic processing unit cards.

As organizations, including those focused on defense, collect larger and more complex sets of data, analysis is becoming a valuable tool for decision making. "We're working with the best people in the world to bring high-performance computing to new problems in the national defense mission and beyond," noted Eric Werner, technical director and chief architect for the ETC.

"We're working with the best people in the world to bring high-performance computing to new problems in the national defense mission and beyond."

—Eric Werner, Emerging Technology Center



"It is a strategic goal for both (ISC)² Pittsburgh and the CERT Division's Cyber Workforce Development Directorate to provide outreach to the community and increase awareness and interest in cybersecurity professions among school students."

—Jonathan Frederick, SEI CERT Division

Rotem D. Guttman

Jonathan Frederick

High School Cybersecurity Competition Part of SEI's 2015 STEM Effort

In July 2015, the SEI CERT Division partnered with the Pittsburgh, Pennsylvania Chapter of the International Information Systems Security Certification Consortium —(ISC)²— to host a cybersecurity workshop and competition for high school students in the Pittsburgh area. The purpose of the three-day event, conducted at the CERT Division's Distributed Learning Center, was to provide high school students an opportunity to interact with cybersecurity experts, learn and practice cybersecurity concepts, and discover potential career options in the field of cybersecurity.

"It is a strategic goal for both (ISC)² Pittsburgh and the CERT Division's Cyber Workforce Development Directorate to provide outreach to the community and increase awareness and interest in cybersecurity professions among school students," said the CERT Division's Jonathan Frederick, vice president of (ISC)² Pittsburgh.

The first half of the event was devoted to educational activities that introduced students to a range of cybersecurity topics, including firewalls, intrusion detection, encryption, access control, insider threat, social engineering, denial-of-service attacks, and incident response. The remainder of the program afforded the students the opportunity to apply their knowledge in game and competition settings.

"'Three Envelopes' is a game designed to place players in the role of corporate CEO," explained the SEI's Rotem Guttman, developer of the game. Guttman designed "Three Envelopes" to be a fun and intuitive way to learn the basics of risk management. "It forces players to make tough decisions about where to invest their company's resources," added Guttman. "Throughout the game, random events occur, such as attempts to steal credit card information, disloyal employees, attempted break-ins, or even economic sanctions. How these events affect each player's company determined what security choices and investments they made."

The students also competed in a realistic "Prioritizing Defensive Measures" competition that pitted teams of students against each other. The teams worked to defend a typical corporate network under attack by hackers in a realistic environment created using the SEI's STEPfwd training platform.

"The student teams used various cybersecurity tools to determine what attacks were taking place," said Frederick. "They then worked to prioritize the attacks based on their severity and secure their network to stop the attacks. The teams scored points based on their ability to maintain key network services necessary to keep their business up and running, and teams lost points when they locked down their networks so much that essential business services were blocked — a realistic scenario that cyber professionals face on a daily basis."

Event organizers were surprised at the students' depth of cybersecurity knowledge. "The teams ended the day with scores similar to those we typically see with graduate-level university student teams working on the same exercise," said Frederick.

This high school cybersecurity competition is part of the SEI's ongoing commitment to STEM education. In addition to Frederick and Guttman, other SEI participants included Robert Beveridge, Chris Herr, Christopher May, Lisa Young, and Nick Winski. All served as instructors during the educational portion of the event.

Christopher King

Dan Klinedinst

Collaboration with U.S. DOT and DHS Aims at Making Government Vehicle Fleets More Secure

Devices that connect cars and trucks to the Internet are revolutionizing how organizations track and run their fleets, but not without a major security risk. While these devices provide valuable data, such as mileage and GPS locations, automobiles themselves were never meant to be connected directly to the Internet, so they don't employ safeguards that prevent adversarial attacks. The vulnerabilities vary, but some are serious and could lead to complete vehicle compromise.

Christopher King, who investigated these devices along with fellow SEI researcher Dan Klinedinst, put it this way: "If you can plug into one of the car's ports, you can make the car do whatever you want."

The SEI is working on ways to guard against that. Collaborating with the United States Computer Emergency Readiness Team (US-CERT) and the Volpe Center at the U.S. Department of Transportation (DOT), SEI researchers examined seven on-board diagnostic devices, such as consumer-connected car adapters and wireless diagnostic code readers, for vulnerabilities that could be exploited. In October 2015, the researchers presented their findings to government fleet managers at the Cybersecurity for Government Vehicles Steering Group. Managers in attendance came from organizations such as the General Services Administration (GSA), which is the head buyer of U.S. government fleet vehicles; the FBI; and the United States Secret Service.

Because all vehicles in the government fleet must integrate telecommunications and information technology (known as telematics), the SEI's next step is testing these mobile hotspot devices on a real car to determine how to make the devices, and in turn the cars they connect to, secure. The DOT borrowed a car for testing from Transport Canada, an organization comparable to the U.S. DOT.

Through reverse-engineering on the test car, the SEI plans to identify security vulnerabilities in these devices and report them to the device manufacturers so the risks can be eliminated. Then, the SEI will make recommendations for how the U.S. government can make its fleet vehicles secure and what the general public should consider before buying one of these devices.

Already this research is making a difference for the U.S. government. According to Tom Millar, chief of communications at US-CERT, who attended the steering group meeting and sponsors this work, "We made a difference today in helping several major fleet managers make better decisions about aftermarket telematics. Multiple agencies, including GSA, repeatedly referred to us [US-CERT and SEI researchers] as a necessary input for future buys."

King thinks the work is going to have a real impact. "The device manufacturers are new to security and have to consider a whole new mindset. Our recommendations will help them do just that."

"If you can plug into one of the car's ports, you can make the car do whatever you want."

—Christopher King, SEI CERT Division

Matt Butkovic

Assessments Help Organizations Secure Critical Infrastructure

Reducing risks associated with third-party dependencies and supply chains, strengthening the resilience of critical infrastructure, identifying and mitigating network vulnerabilities—this work is what the SEI CERT Division's Cybersecurity Assurance team is all about. "Our goal is to help key business and government sectors better protect essential systems from cyber threats and disruptions," said Matt Butkovic, the team's technical manager. "To meet it, we expanded our programs considerably this year."

External Dependencies Management Assessments

In 2015, the Cybersecurity Assurance team and the Department of Homeland Security (DHS) launched the External Dependencies Management (EDM) Assessment. This in-person, DHS-facilitated evaluation measures how well an organization can handle cyber disruptions in key services provided by third parties. Any external dependency presents a risk, from service agreements for cloud computing to business relationships that depend on a third party's computing infrastructure and security.

Cyber Resilience Reviews

Protecting critical national infrastructure such as energy, water, transportation, and financial systems from cyber disruptions was also on the Cybersecurity Assurance team's agenda. During 2015, it conducted 48 Cyber Resilience Reviews (CRRs) in 10 critical infrastructure sectors. A CRR evaluates an organization's operational resilience and cybersecurity practices in 10 domains, including risk management, incident management, and service continuity. It's a no-cost, voluntary, non-technical assessment of enterprise-wide threats that can be self-administered or conducted by DHS cybersecurity professionals. Organizations get a detailed, actionable list of suggestions for improving their resilience. As of the end of the 2015 fiscal year, the SEI's CERT Division had facilitated 359 CRRs.

Organizations did not perform equally well across all of the domains in the CRR. While organizations on average did a good job managing their assets, change, and external dependencies, they did not do as well in overall risk management, training, and situational awareness. By identifying areas in which organizations are most vulnerable, the CRR points the way to improved resilience.

Risk and Vulnerability Assessments

Recent data breaches in industry and government agencies have shown how vulnerable even tech-savvy organizations are to cyber attacks. Risk and Vulnerability Assessments (RVAs) help organizations understand their cyber vulnerabilities and determine whether their current security practices protect against them. During 2015, the Cybersecurity Assurance group worked with the DHS to conduct 46 RVAs. Overall, organizations are getting better at protecting their websites in the face of distributed denial of service (DDoS) attacks and other website breaches. However, they are still plagued by phishing attempts, which continued to be the most widespread and visible method of attack.

For more information on the CERT Division's work on assessment and resilience, visit cert.org/resilience.

Steve Beck

Helping the Marine Corps Lay the Groundwork for Systems Modernization

Ask Steve Beck of the Software Engineering Institute to describe 2015 in one word, and he doesn't hesitate one bit. "Epic." And Beck knows what he's talking about.

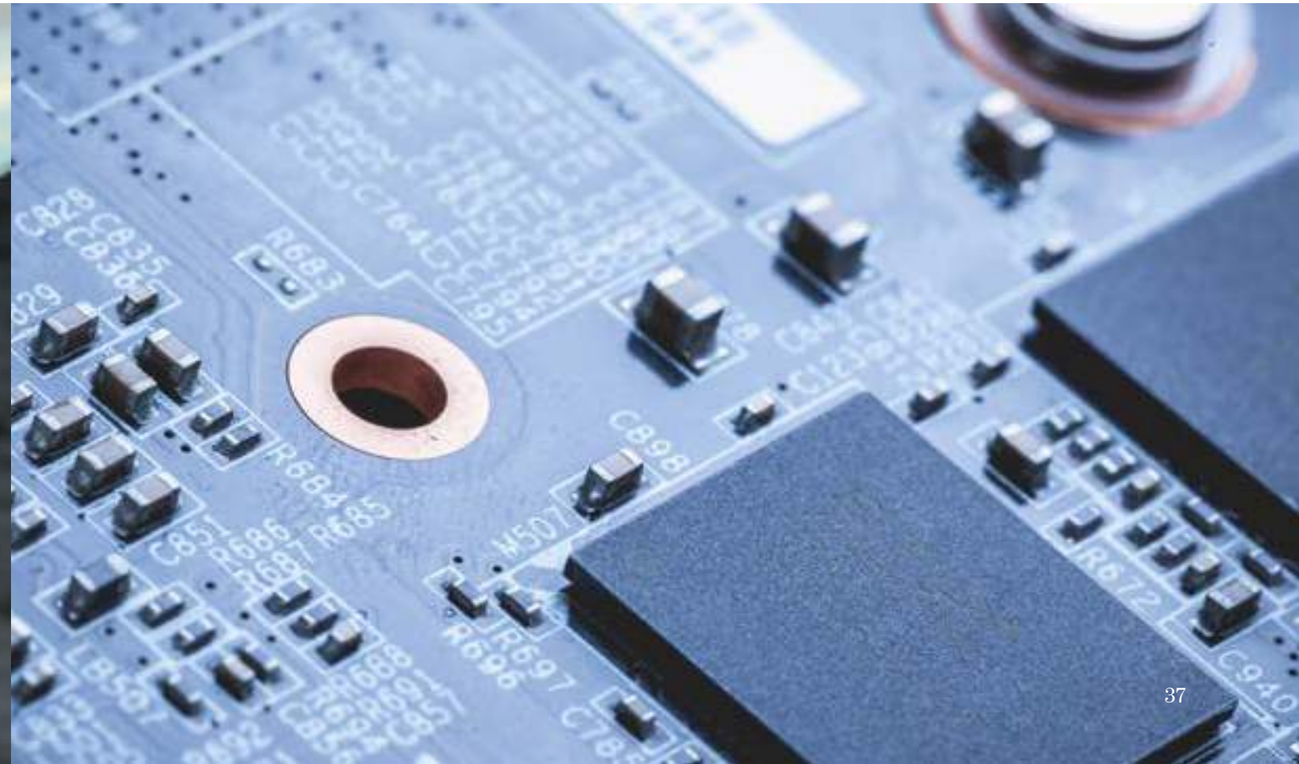
Beck is referring to the Enterprise Portfolio IT Integration and Information Center for Systems of Systems Engineering, or EPI³CS. This center is the first foundational phase of a major program to modernize and integrate Marine Corps IT systems development within existing portfolios. The effort brought together the SEI and other federally funded research and development centers, university-affiliated research centers, government laboratories, academia, military academies, and war colleges to design and build a consolidated development infrastructure, streamline processes, and develop the software engineering workforce.

Beck noted the EPI³CS team will evaluate and analyze Marine Corps systems, subsystems, and applications in a disciplined, systematic manner. Reports based on this work will give Marine Corps leadership the requisite system engineering rigor to support complex portfolio management decisions.

Last year was the "design and construct" year for EPI³CS. The SEI will again play a key role in 2016, shifting its effort to establishing and operating the ESI²—the Enterprise System of Systems Engineering Integration and Innovation Environment. At that stage, the team will perform system design experiments and demonstrations.

"The Marine Corps has embarked upon an aggressive campaign to modernize its defense business systems in order to meet today's and tomorrow's threats," said Al Wincek, the Marine Corps Business Mission Area Chief Engineer and primary sponsor of the effort. "We have enlisted the help of the SEI to accomplish this, and the results have been significant and have received support from the highest levels of Marine Corps leadership."

Photo: U.S. Marine Corps



TRANSITION

The SEI accelerates the impact of software and cybersecurity improvements by working to promote adoption of improved capabilities by the defense industrial base and the wider software and cybersecurity communities. The SEI does this by creating standards, prototypes and tools, technical guidance, and platforms for knowledge and skill acquisition.

Standards

The SEI develops standards that improve the software ecosystem on which the Department of Defense (DoD) relies. For instance, the CERT Secure Coding Initiative has been leading the community development of secure coding standards for common programming languages. Many of these proposed practices are in use by major participants in the supply chain for DoD software-reliant systems, including Cisco Systems and Oracle. The SEI has also worked to integrate several research technologies into the Architecture Analysis and Design Language standard, making it extensible and semantically well defined. Application of the standard promotes the virtual integration of system building and testing activities—an approach that supports DoD objectives of achieving integrated warfighting capabilities and delivering solutions sooner to warfighters.

Prototypes and Tools

SEI researchers develop software prototypes that test proposed solutions, like the smartphone app developed in collaboration with the Carnegie Mellon University Human-Computer Interaction Institute. Called the Edge Mission-Oriented Tactical App Generator (eMONTAGE), this software program for mobile devices enables warfighters to mash data from multiple sources and view the results on a unified display—all without writing code. SEI researchers have demonstrated an eMONTAGE prototype at the U.S. Special Operations Command/Naval Postgraduate School (NPS) Tactical Network Testbed and at NPS's Joint Interagency Field Exploration (JIFX).

Tools

The SEI systematically builds software tools, especially those that address acute cybersecurity needs. Fuzz-testers and debuggers developed by the SEI's CERT Division, for example, can position military software engineers to meet requirements outlined in the 2013 National Defense Authorization Act for software assurance testing. Other SEI tools facilitate security analysis in large networks, enable analysts to rapidly query large sets of data traffic volumes, process packet data into bidirectional flow records, and simplify the building of analysis environments.

Technical Guidance, Workforce Development, and Knowledge Sharing

The SEI shares the progress and results of its research through a host of media avenues, including

- technical reports, blog entries, webinars, and podcasts available on its websites
- articles in prestigious professional journals and in publications geared to practitioners
- books in the SEI Series in Software Engineering published by Addison-Wesley

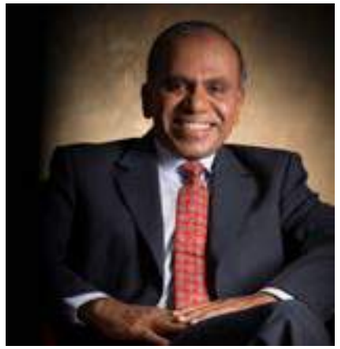
Those books often form the basis for education materials and training courses offered by the SEI and others. The SEI offers classroom and eLearning courses in software acquisition, network security, insider threat, software architecture, software product lines, software management, and other areas.

In 2012, the SEI introduced the CERT STEPfwd (Simulation, Training, and Exercise Platform) to help cybersecurity practitioners and their teams continually build knowledge, skills, and experience.

In addition, SEI researchers collaborated with educators from around the United States to develop the first curriculum for software assurance, the Master of Software Assurance (MSwA). The IEEE Computer Society and Association for Computing Machinery, as well as community leaders in curriculum development, formally recognized the MSwA Reference Curriculum as suitable for creating graduate programs or tracks in software assurance.

LEADERSHIP

Carnegie Mellon University Leadership



Subra Suresh
President
Carnegie Mellon University

Farnam Jahanian
Provost
Carnegie Mellon University

SEI Executive Leadership Team

Seated: David Thompson, Chief Information Officer; Robert Behler, Deputy Director and Chief Operating Officer; Kevin Fall, Deputy Director and Chief Technology Officer; Mary Catherine Ward, Chief Strategy Officer

Standing: Matthew E. Gaston, Director, SEI Emerging Technology Center; Peter Menniti, Chief Financial Officer; Paul Nielsen, Director and Chief Executive Officer; Richard Pethia, Director, CERT Division; John Bramer, Chief of Staff; Edward Deets, Director, Software Solutions Division

Organization

SEI Director's Office

Paul D. Nielsen
Director and Chief Executive Officer

Robert Behler
Deputy Director, Chief Operating Officer

Kevin Fall
Deputy Director, Chief Technology Officer

Software Solutions Division

Edward Deets
Director

Anita Carleton
Deputy Director

David Zubrow
Chief Scientist (Acting)

CERT Division

Richard Pethia
Director

Bill Wilson
Deputy Director

Greg Shannon
Chief Scientist

Emerging Technology Center

Matthew E. Gaston
Director

Eric B. Werner
Deputy Director

Office of the Chief of Staff

John Bramer
Chief of Staff

David Thompson
Chief Information Officer

Financial And Business Services

Peter Menniti
Chief Financial Officer

Strategic Initiatives

Mary Catherine Ward
Chief Strategy Officer

SEI Legal

Sandra Brown
SEI General Counsel

Board of Visitors

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

Barry W. Boehm
TRW Professor of Software Engineering, University of Southern California; Director, University of Southern California Center for Software Engineering

John M. Gilligan
President, Gilligan Group; former Senior Vice President and Director, Defense Sector of SRA International; former CIO for the Department of Energy

Alan J. McLaughlin
Chair, Board of Visitors; Consultant; Former Assistant Director, MIT Lincoln Laboratory

Gilbert F. Decker
Consultant; former President and CEO, Penn Central Federal Systems Company; former President and CEO of Acurex Corporation; former Assistant Secretary of the Army/Research, Development, and Acquisition

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

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

Philip Dowd
Private Investor; former Senior Vice President, SunGard Data Systems; Trustee, Carnegie Mellon University

Tom Love
Chief Executive Officer, Shoulders Corp; Founder of Object Technology Group within IBM Consulting

SEI STAFF

Full-Time & Part-Time Staff and Other Contributors

Lisa Abel
Steve Ader
Laura Aguera
Cecilia Albert
Christopher Alberts
Michael Albrethsen
William Aldrich-Thorpe
Dennis Allen
Noelle Allon
Amanda Alvarez
Gregory Anderson
Laura Anderson
William Anderson
Bjorn Andersson
Eileen Angulo
Christopher Antalek
John Antonucci
Luiz Antunes
Jeffrey Apolis
Melissa Argenziano
Leena Arora
Christopher Atwood
Eric Azebu
Felix Bachmann
Marie Baker
Karen Balistreri
Vincent Balistreri
Aaron Ballman
Jeffrey Balmert
Ronald Bandes
Michael Bandor
Hollen Barmer
Peter Barrett
Jeffrey Basista
Barbora Batokova
Daniel Bauer
Christopher Baum
Roger Beard
Dwight Beaver
Stephen Beck
Robert Behler
David Belasco
Stephany Bellomo
Jonathan Bender
Brian Benestelli
Kate Bennett
Kristi Berneburg
Shawn Besselman
James Besterci
Robert Beveridge
Philip Bianco
David Biber
Daniel Bidwa
Darlene Bigos
Tracy Bills
Robert Binder
Marla Blake
Stacie Blakley
Stephen Blanchette
Jeffrey Boleng
Elaine Bolster
Randall Bowser
Andrew Boyd
Diane Bradley
Ben Bradshaw
John Bramer
Kara Branby
Pamela Brandon
Heidi Brayer
Scotty Brennan
Lea Bridi
Rex Brinker
Rita Briston
Rhonda Brown
Lisa Brownsword
Andrew Bunker
John Bush
Matthew Butkovic
Palma Buttles-Valdez
Anthony Calabrese
Rachel Callison
Sara Cammarata
Kimberley Campbell
Linda Campbell
Linda Canon
Peter Capell
Anita Carleton
Cassandra Carricato
William Casey
Kelly Cassidy
Anthony Cebzanov
Sagar Chaki
Mary Jo Chelosky
Timothy Chick
Leslie Chovan
Mary Beth Chrissis
Natalie Chronister
Jonathan Chu
Matthew Churilla
Jason Clark
Kathleen Clarke
William Claycomb
Matthew Coates
Cory Cohen
Julie Cohen
Sanford (Sholom) Cohen
Mary Lou Cole
Matthew Collins
Anne Connell
Carol Connelly
John Connelly
Robert Conway
Michael Cook
Stephen Cooney
Rebecca Cooper
Stephanie Corbett
Alexander Corn
Daniel Costa
Jennifer Cowley
Susan Cox
Randy Crawford
Rita Creel
Lucy Crocker
Larry Crowe
Stephanie Crowe
Michael Crowley
Natalie Cruz
Pamela Curtis
Jerome Czerwinski
Rebecca D'Acunto
Roman Danyliw
Rosemary Darr
Jeff Davenport
John Dayton
Dionisio De Niz
Edward Deets
Grant Deffenbaugh
Julien Delange
Kareem Demian
Matthew Desantis
Edward Desautels
Aaron Detwiler
Jill Diorio
John Diricco
Robert Ditmore
Mary Dixon
Geoff Dobson
Patrick Donohoe
William Dormann
Audrey Dorofee
Margie Drazba
Elke Drennan
Michael Duggan
Catherine Duncan
Evelyn Duncan
Madelaine Dusseau

Ladonna Dutton
Karin Dwyer
Sean Easton
James Edmondson
Danielle Edwards
Eileen Eicheldinger
Robin Eisenhart
Linda Elmer
Harold Ennulat
Lover Epps
Neil Ernst
Felicia Evans
Sidney Faber
Michele Falce
Kevin Fall
Kimberly Farrah
Mariane Fazekas
Jeffrey Federoff
Peter Feiler
Eric Ferguson
Constance Ferra
Donald Firesmith
Kodiak Firesmith
Brendan Fitzpatrick
Lori Flynn
Justin Forbes
John Foreman
Kunta Fossett
Arne Fostvedt
Summer Fowler
Tracey Fox
Jonathan Frederick
David French
Michelle Fried
Michael Fritz
Brent Frye
Michael Gagliardi
Brian Gardiner
Douglas Gardner
Matthew Gaston
Linda Parker Gates
David Gearhart
Jeffrey Gennari
Stephen Gifford
Lisa Gillenwater
Ryan Gindhart
Jamie Glenn
Walter Goss
Wassie Goushe
Bruce Grant
Douglas Gray
Michael Greenwood
Russell Griffin
Phillip Groce
Jacqueline Grubbs
Rajasekhar Gudapati
Arie Gurfinkel
Rotem Guttman
David Guzik
Shannon Haas
Bart Hackemack
Nancy Hags
John Haller
William Halpin
Jeffrey Hamed
Josh Hammerstein
Jeffery Hansen
Stephen Hardesty
Kimberly Hardin
Erin Harper
Jeffrey Havrilla
Jason Hawk
William Hayes
Matthew Heckathorn
Jessica Hedges
Stephanie Hedges A
Sharon Henley
Christopher Herr
Donald Hess Charles
Hines Scott Hissam
Barbara Hoerr Bryon
Holdt Charles
Holland Andrew
Hoover Angela
Horneman Allen
Householder Joshua
Howell Ryan Howley
John Huber
John Hudak
Clifford Huff
Lyndsi Hughes
Jennifer Hykes
Chris Inacio
Terry Ireland
James Ivers
Jerry Jackson
Vanessa Jackson
Michael Jacobs
Michael Jehn
William Jones
Jacob Joseph
Patricia Junker
Gavin Jurecko
Matthew Kaar
Stephen Kalinowski
Rachel Kartch
Mark Kasunic
Harry Kaye
David Keaton
Tracey Kelly
Robert Kemerer
Brent Kennedy
Jennifer Kent
Carolyn Kernan
Christopher King
Kimberly King-Cortazzo
John Klein
Mark Klein
Stacy Klein
Mark Klepach
William Klieber
Dan Klinedinst
Georgeann Knorr
Andrew Kompanek
Michael Konrad
Keith Korzec
Paul Krystosek
Robert Kubiak
Amy Kunkle
Zachary Kurtz
David Kyle
Michael Lambert
Joel Land
Debra Lange
Mark Langston
Mary Ann Lapham
Vincent Lapiana
Frank Latino
David Law
Alyssa Le Sage
Bernadette Ledwich
Ryan Lehman
Harry Levinson
Todd Lewellen
Darrell Lewis
Grace Lewis
Alena Leybovich
Amy Leyland
Braden Licastro
Joshua Lindauer
Martin Lindner
Howard Lipson
Reed Little
Todd Loizes
James Lord
Melissa Ludwick
Richard Lynch
Rudolph Maceyko
Harold Major
Lisa Makowski
Arthur Manion
Jay Marchetti
Attilio Marini
Tamara Marshall-Keim
Theodore Marz
Lisa Masciantonio
Laura Mashione
Michael Massa
Joseph Matthews
Roxanne Matthews
Jeffrey Mattson
Christopher May
Joseph Mayes
John McAllister
Michael McCord
James McCurley
Patricia McDonald
Roy McDonald
Michelle McGee
Shane McGraw
James McHale

David McIntire
Donna McIntyre
Donald McKeon
Janis McKinney
Bernadette McLaughlin
Michael McLendon
Joseph McLeod
Scott McMillan
Jason McNatt
Deborah McPherson
Nancy Mead
Ryan Meeuf
Nader Mehravari
Andrew Mellinger
Peter Menniti
Thomas Merendino
Jennifer Mersich
Leigh Metcalf
Bryce Meyer
Toby Meyer
Bertram Meyers
Amy Miller
Cassandra Miller
Gerald Miller
Suzanne Miller
Samantha Misurda
Soumyo Moitra
Elizabeth Monaco
Austin Montgomery
Andrew Moore
Jose Morales
Damon Morda
Gabriel Moreno
John Morley
Edwin Morris
Timothy Morrow
Anna Mosesso
Angela Mosqueda
Jamie Moyes
David Murphy
Paul Murray
Mark Musolino
Min Young Nam
Cynthia Nesta
Gail Newton
William Nichols

Paul Nielsen
Crisanne Nolan
Robert Nord
Mika North
William Novak
Marc Novakouski
Kevin Nowicki
Jasmine Oates
Sharon Oliver
Kyle O'Meara
Nancy Ott
James Over
Ipek Ozkaya
Mari Palestra
Timothy Palko
Mark Palmquist
Amanda Parente
Allison Parshall
Carmal Payne
David Pekular
Kelwyn Pender
Brenda Penderville
Samuel Perl
Sharon Perry
Richard Pethia
Alexander Petrilli
Thomas Petrus
David Phillips
Janet Philpot
Kevin Pitstick
Patrick Place
Daniel Plakosh
Michael Pochan
Thomas Podnar
Shauna Policicchio
William Pollak
Stephanie Pomerantz
Mary Popeck
Jason Popowski
Douglass Post
Jerome Pottmeyer
Katherine Prevost
Andrea Prilla
Sean Provident
Kara Quinto
Traci Radzyniak

Angela Raible
James Ralston
Donald Ranta
Michael Rattigan
Frank Redner
Sonia Reed
William Reed
Aaron Reffett
Colleen Regan
Nicholas Reimer
David Reinoehl
Janet Rex
Clifford Rhoades
Louis Richards
Nathaniel Richmond
Michael Riley
Stacey Rizzo
John Robert
Lawrence Rogers
James Root
Robert Rosenstein
Sheila Rosenthal
Dominic Ross
Adam Rousseau
Bradley Rubbo
Daniel Ruef
Robin Ruefle
Brad Runyon
Kristopher Rush
Mary Lou Russo
Mary Lynn Russo
Charles Ryan
Samuel Salinas
Venkatavijaya Samanthapudi
Thomas Sammons
Geoffrey Sanders
Concetta Sapienza
Emily Sarneso
Vijay Sarvepalli
Jeff Savinda
Thomas Scanlon
Alfred Schenker
David Scherb
Robert Schiela
Andrew Schlackman
Steve Scholnick

Patricia Schreiber
James Schubert
Leslie Schuch
Carol Schultz
Kenneth Schultz
Edward Schwartz
Giuseppe Sciulli
Tina Sciullo-Schade
Philip Scolieri
David Scott
Shirley Scott
William Scully
Johnathan Seaburn
Joseph Seibel
James Semler
Gregory Seroka
Gregory Shannon
Sharon Shaw
Sarah Sheard
David Shepard
Mark Sherman
Nataliya Shevchenko
Deana Shick
Timothy Shimeall
Linda Shooer
Sandra Shrum
Forrest Shull
George Silowash
Matthew Sisk
Lisa Sittler
Danica Slater
Carol Sledge
Michelle Slusser
James Smith
Holly Smith
Lenny Smith
Timur Snoke
Benjamin Solecki
Gabriel Somlo
Tara Sparacino
Debra Spear
James Spencer
Derrick Spooner
Jonathan Spring
Bryan Stake
Lauren Stanko

Jonathan Steele
Lizann Stelmach
Katie Stewart
Robert Stoddard
John Stogoski
Michael Stone
Edward Stoner
Jeremy Strozer
Gregory Such
Siobhan Sullivan
David Svoboda
Michael Szegedy
Lucille Tambellini
Joe Tammariello
Michael Theis
Marcia Theoret
Jeffrey Thieret
Kimberly Thiers
Alisa Thomas
Mark Thomas
William Thomas
David Thompson
David Tobar
Michele Tomasic
Barbara Tomchik
Carolyn Tomko
Patsuda Tonburintrtipye
Brian Torbich
Helen Trautman
Peter Troxell
Donovan Truitt
Randall Trzeciak
Laurie Tyzenhaus
David Ulicne
Jeanette Urbanek
Vijay Vadlamudi
Justin Valdengo
Christine Van Tol
Satya Venneti
Joseph Vessella
Aaron Volkmann
Alexander Volynkin
Robert Vrtis
Todd Waits
Kurt Wallnau
Cynthia Walpole

Pennie Walters
Rand Waltzman
Mary Ward
David Warren
Trina Washington
Garret Wassermann
Rhiannon Weaver
Samuel Weber
Charles Weinstock
Adam Welle
Eric Werner
James Wessel
Austin Whisnant
Barbara White
Amanda Wiehagen
Akia Williams
Keegan Williams
Pamela Williams
William Wilson
Craig Wink
Nicholas Winski
Robert Wojcik
Brandon Wolfe
William Wood
Carol Woody
Lutz Wrage
Evan Wright
Michael Wright
Joseph Yankel
Charles Yarbrough
John Yarger
Hasan Yasar
Jamie Yoder
Lisa Young
Cat Zaccardi
Mark Zajicek
Gene Zambrano
Marianne Zebrowski
John Zekany
David Zubrow
Allison Zust

Other Contributors

Elyse Azzato
Nanette Brown
Sandra Brown
Lisa Depasquale
Angel Jordan
Kenneth Nidiffer
Christine Zobel
Julia Allen
Brian Averi
Donald Beynon
Grady Campbell
Tracy Cassidy
Peter Chen
Robert Ellison
Luis Figueroa
Dennis Goldenson
John Goodenough
Charles Hammons
Eric Hatleback
Frederick Kazman
Sung Lee
Joseph McManus
Julia Mullaney
Linda Northrop
William Scherlis
Doug Schmidt
Lui Sha
Eileen Wrubel

Affiliates

Yoshihiro Akiyama
Yasutaka Shirai
Diego Vallespir

Copyright

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

No Warranty

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.

Use, Distribution, and Service Marks

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 marks of Carnegie Mellon University.

EPIC℠

DM-0003543

Manager, Communication Services
William Thomas

Manager, Public Relations
Richard Lynch

Manager, Corporate & Technical Communications
Janet Rex

Editor-in-Chief
Ed Desautels

Editorial
Hollen Barmer
Heidi Brayer
Ed Desautels
Claire Dixon
Erin Harper
Tamara L. Marshall-Keim
Gerald Miller
Nancy Ott
Sandra Shrum
Pennie Walters
Barbara White

Design
Christopher Baum

Illustration
Kurt Hess

Digital Production
Mike Duda

Photography
David Biber
Ed Desautels
Tim Kaulen, Photography and Graphic Services, Mellon Institute

Web Design
Barbora Batokova

SEI Pittsburgh, PA
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

SEI Washington, DC
Suite 200
4301 Wilson Boulevard
Arlington, VA 22203

SEI Los Angeles, CA
2401 East El Segundo Boulevard
El Segundo, CA 90245