Carnegie Mellon University Software Engineering Institute (SEI) Overview

Mary Catherine Ward

Chief Strategy Officer

The SEI is a DoD R&D Federally Funded Research and Development Center

Established in 1984 at Carnegie Mellon University

~615 employees (ft + pt), of which about 70% are engaged in technical work

Initiated CERT cybersecurity program in 1988

Primary offices in Pittsburgh and DC, with several operating locations near customer facilities

About $150M in funding
(~$20M DoD Appropriated Line)

DoD FFRDCs: Strategic Capability Maintained through a Special Contractual Relationship

Meet a need that cannot be met as effectively with existing in-house or contractor resources

Granted access *beyond that of a typical contractor relationship* to government and supplier data, sensitive and proprietary information, personnel, and facilities

Operate in the public interest with objectivity and independence, free from organizational conflicts of interest

Required to conduct business in a non-profit manner befitting its special relationship with the government

Undergo a comprehensive review by government sponsor every five years

DoD FFRDCs: Support Government Research, Technology Development, and Systems Acquisition

"FFRDCs assist in transferring technology between the government and the private sector by promoting development of new technologies. …[They are] a repository for knowledge accessible to the U.S. government and industry unencumbered with conflicts concerning for-profit institutions."

"U.S. Science and Technology Leadership, and Technology Grand Challenges"
in *Synesis, A Journal of Science, Technology, Ethics, and Policy*,
Robert Hummel, Patrick Cheetham, and Justin Rossi, 2012

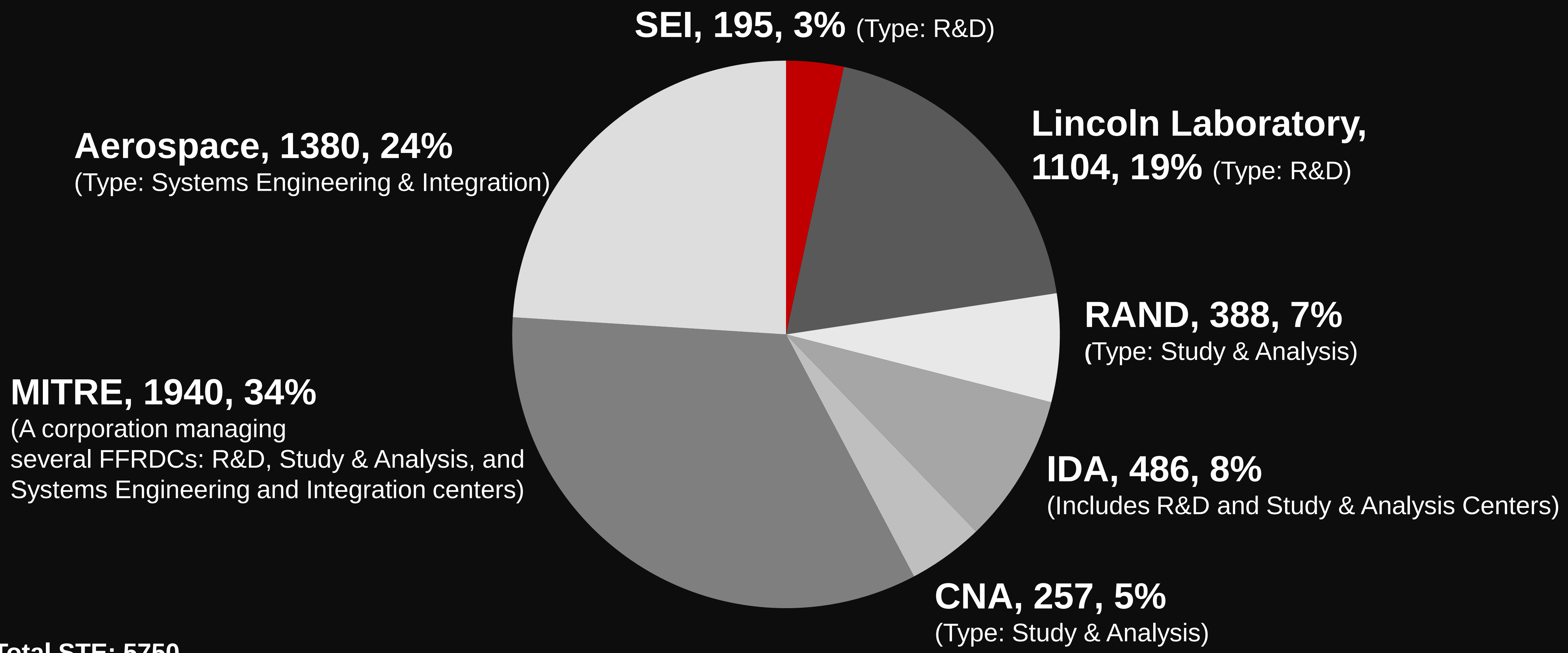
Provide creative and cost-effective solutions to government problems of considerable complexity

Analyze technical questions with a high degree of objectivity

Three activity types:

- R&D
- Study & Analysis
- Systems Engineering and Integration

DoD FFRDCs: Initial FY17 STE Allocations



Total STE: 5750

The SEI is the only FFRDC charged to improve the state of the art and practice of software engineering

Our Leadership


Paul D. Nielsen
Director and CEO


Robert Behler
Deputy Director
and COO


Jeff Boleng
Acting CTO

CERT Division


Roberta Stempfley
Director


Bill Wilson
Deputy Director


Greg Shannon
Chief Scientist

Software Solutions Division


John Bramer
Acting Director


Anita Carleton
Deputy Director


Charles Holland
Chief Scientist

Emerging Technology Center


Matthew E. Gaston
Director


Brenda Penderville
Acting Deputy Director

Chief Strategy Officer


Mary Catherine Ward

CFO


Peter Menniti

General Counsel


Sandra Brown

CIO


David Thompson

Chief of Staff


John Bramer

We Serve a Broad Spectrum of Stakeholders

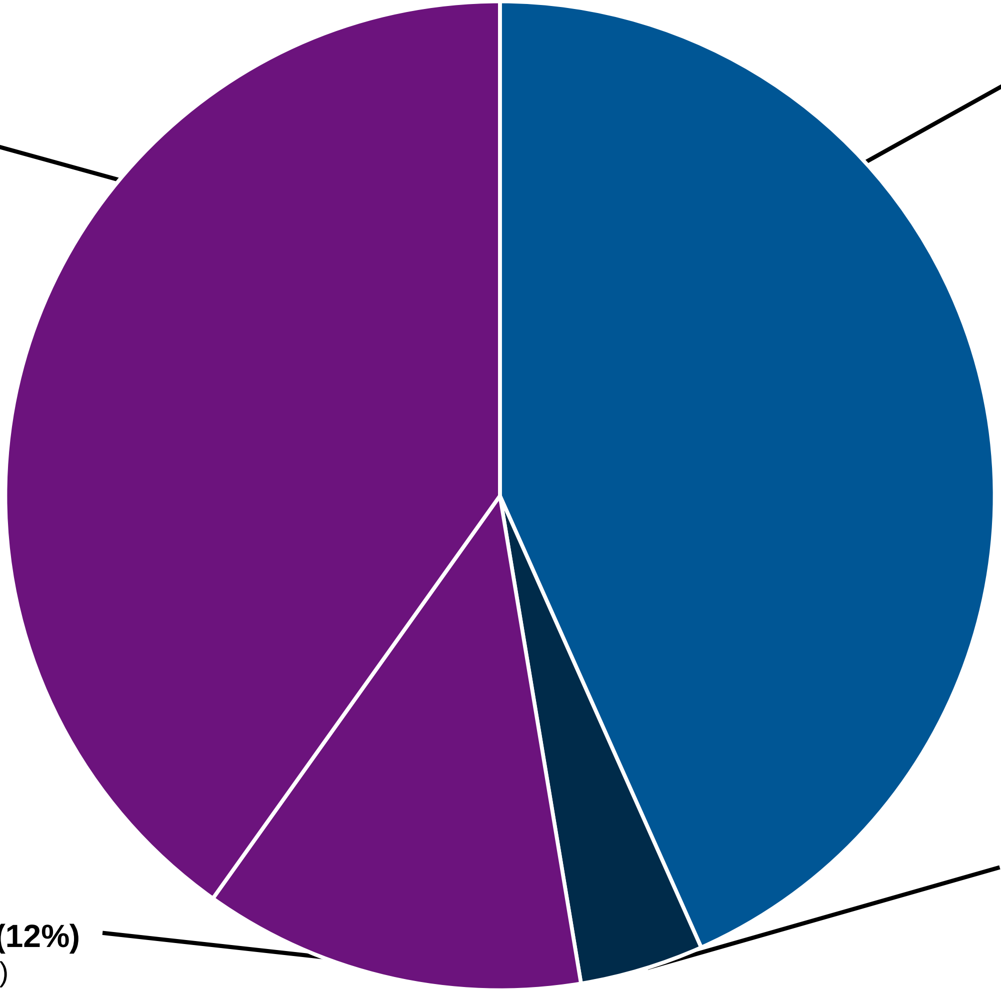
Major government customers

- U.S. DoD
- U.S. DHS

Researchers, developers, users, and acquirers—government, commercial, and academic

Key industries and organizations with the potential to advance software engineering and related disciplines

Our FY17 Work Program Funding Projection ($150.6M)



DoD, $60.5M (40%)

- Air Force ($23.5M)
- Navy & Marine Corps ($14.4M)
- Army ($7.7M)
- US Cyber Command ($4.2M)
- DISA ($3.6M)
- OSD ($2.1M)
- DARPA ($1M)
- DoD Cyber Crime Center ($0.9M)
- MDA ($0.9M)
- Special Ops Command ($0.6M)
- NSA ($0.5M)
- Joint Improvised-Threat Defeat Organization ($0.2M)
- Office of the Director for National Intelligence ($0.2M)
- National Reconnaissance Office ($0.2M)
- ITL, ERADC ($0.2M)
- JTNC ($0.2M)

Federal Agency, $65.3M (44%)

- DHS-Network Security Deployment ($13.5M)
- DHS-Federal Network Resilience ($10.8M)
- DHS-National Cyber Security and Integration Center ($10.1M)
- DHS-Stakeholder Engagement & Cyber Infrastructure Resilience ($8.0M)
- U.S.P.S ($7.4M)
- DHS-U.S. Secret Service ($3.5M)
- DHS-Chief Technology Officer ($3.3M)
- IARPA ($2.3M)
- Department of Energy ($1.5M)
- CIA ($1.5M)
- DHS-Office of the Chief Security Officer ($1.4M)
- Department of Justice ($1.3M)
- Department of State ($0.70M)

DoD OSD, 18.8M (12%)

- OSD Line ($18.8M)

Commercial, $6.0M (4%)

- Education & Training Agreements ($3.2M)
- Work Agreements ($2.8M)

Software is Responsible for Greater System Functionality and Desired Qualities

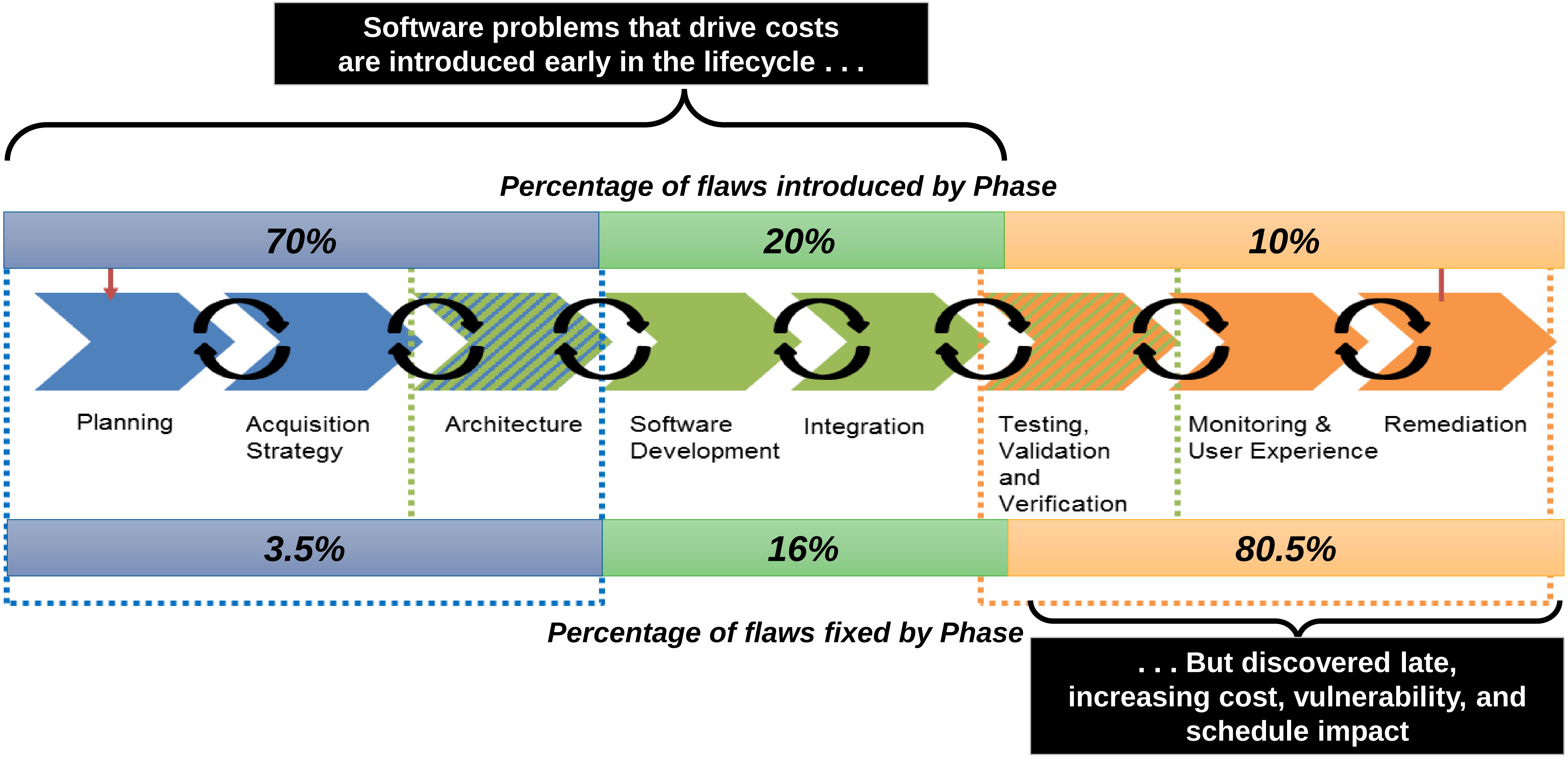
Software can offer

- Reliability
- Adaptability
- Affordable sustainment
- Interoperability
- Interconnectivity

However, software cost and vulnerability threaten military capability

- Finding and fixing software problems late in the acquisition lifecycle drives up cost and delays delivery
- Latent cyber vulnerabilities and those exposed during operations or due to underlying dependencies put missions at risk

Fixing Problems Late Drives Costs, Delays Deployment



We Improve Software-based System Development, Operation, and Sustainment

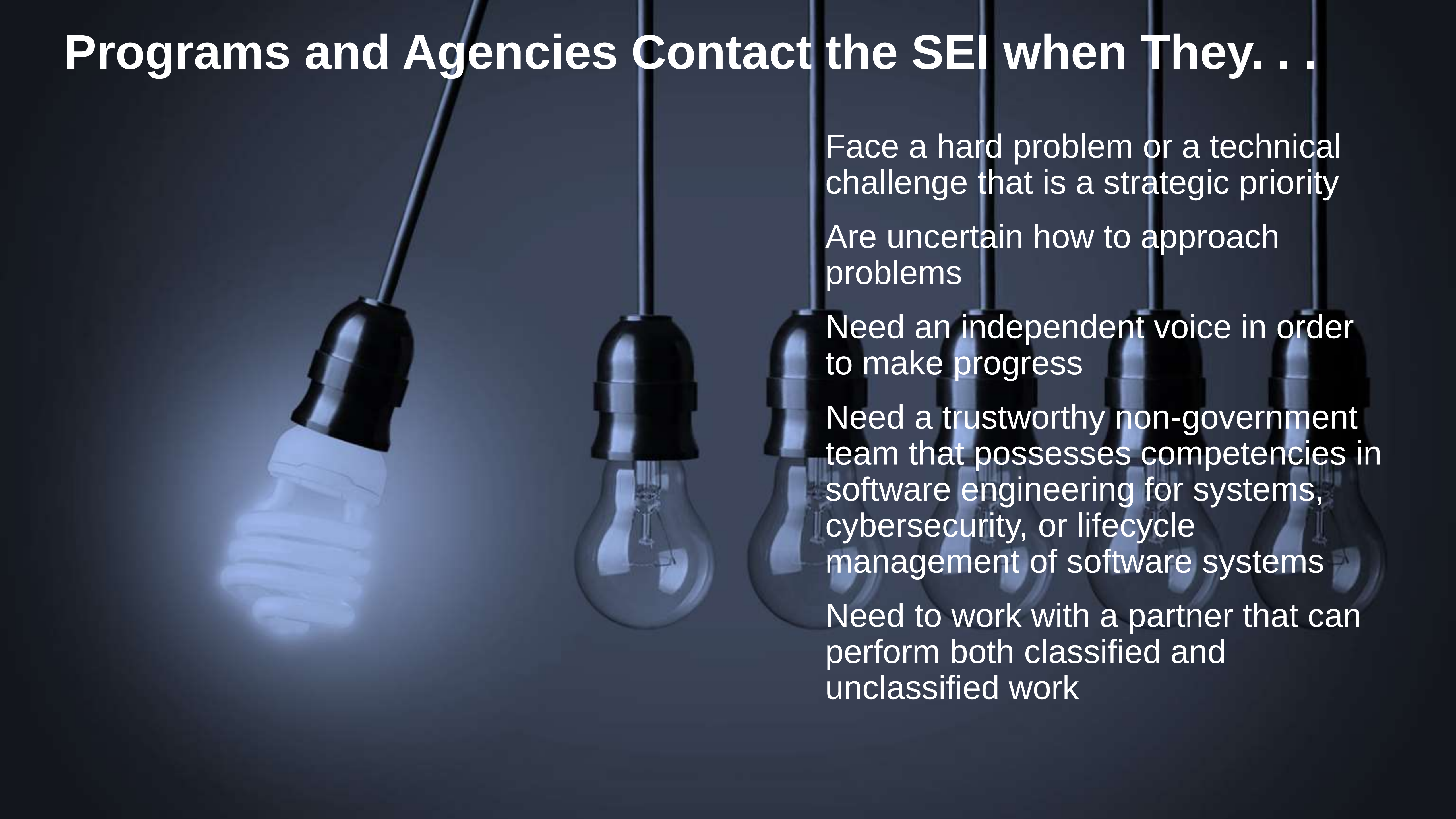
Bend the cost curve of acquiring and sustaining software systems

Rapidly **exploit software-based innovation** to improve the ability to conduct missions

Improve system **assurance and resilience**

Drive research into operations through

- Following guidance from OSD (e.g., Reliance 21 CoIs)
- Creating and prototyping algorithms, tools, technologies, and practices
- Collaborating with Programs and agencies
- Transitioning results to build organic software and cybersecurity capabilities



Programs and Agencies Contact the SEI when They. . .

Face a hard problem or a technical challenge that is a strategic priority

Are uncertain how to approach problems

Need an independent voice in order to make progress

Need a trustworthy non-government team that possesses competencies in software engineering for systems, cybersecurity, or lifecycle management of software systems

Need to work with a partner that can perform both classified and unclassified work

Overview of SEI Facilities

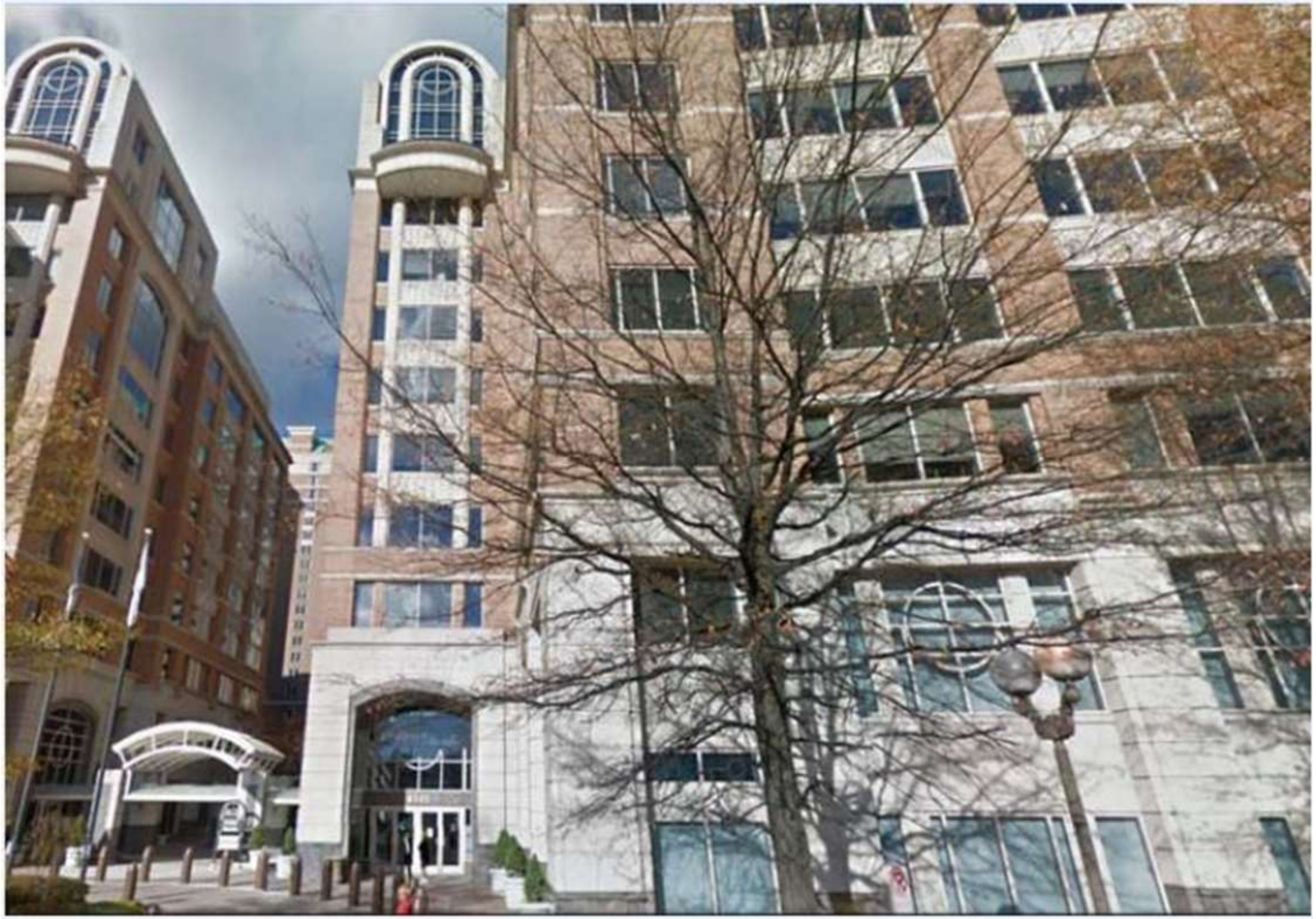
Harry Kaye

Deputy CFO

SEI Maintains Offices in Six U.S. Cities

SEI Based in Pittsburgh – Four Locations

SEI Presence in Arlington, VA



Operating Locations

Leasing small office space in

- Patuxent River, MD
- Burlington, MA
- El Segundo, CA

<u>On customer site – Randolph Air Force Base</u>

- San Antonio, TX

Questions ?

Backup slides

Software Vulnerabilities put Missions at Risk

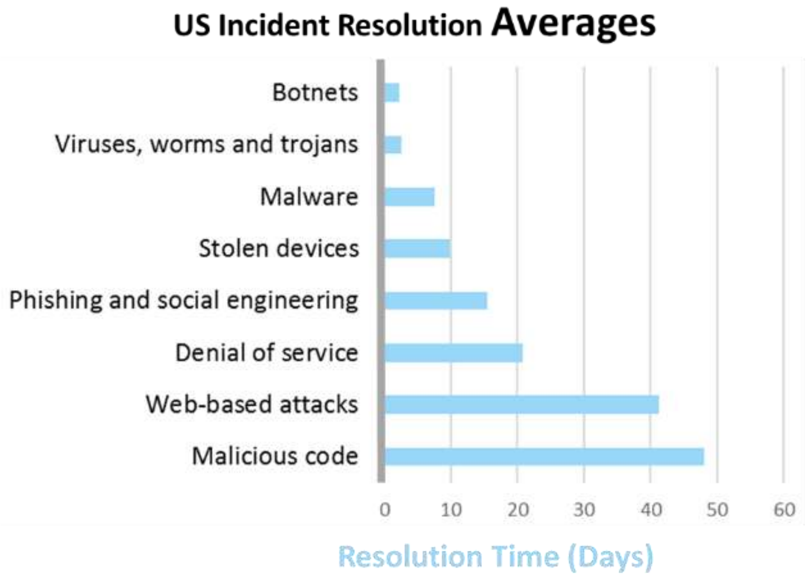
Latent Vulnerabilities

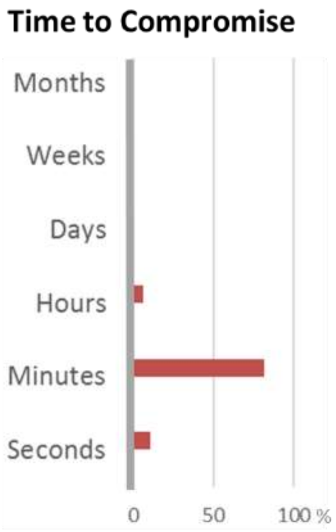
A 10M LOC Weapons Platform written in C will be delivered with 280 – 1,400 exploitable vulnerabilities

- 1 year after operation, 55% of these vulnerabilities will remain
- In sustainment, new vulnerabilities will be introduced

Quality Data: *Capers Jones, NamCook Analytics, 2012*
Vulnerability Data: *SEI, Predicting Cybersecurity Using Quality Data, 2015 IEEE International Symposium on Technologies for Homeland Security*

Cyber Operations Response Lags





< 1 hour is the execution time of the vast majority (86%) of adversary offensive cyber maneuvers

4 – 47 days is the average resolution time for defensive response and mitigation

Incident Resolution Data: *Ponemon Institute and HP Enterprise Security, 2015*
Compromise Time Date: *Verizon Breach Report 2016*

We Work in Seven Core Technical Areas

Enduring

Software Engineering & Information Assurance

Enable high quality, secure software-based systems in a predictable, affordable manner

Cyber Security

Develop improved systems, repeatable practices, and capable personnel to enable cyber missions

System Verification & Validation

Enhance confidence in the systems engineering lifecycle with evidence-based methods and tools

Make software less costly and more resilient and mission capable by ruthlessly automating all aspects of design, development, integration, testing, deployment, operations, defense, and sustainment of software systems

Emerging

Data Modeling & Analytics: Develop and apply mathematically rigorous data collection, analysis, and visualization techniques

$$\hat{p} = \frac{1}{N}\sum_{i=1}^{N} I_{M\circ\Phi}(\vec{X}_i)$$

C4ISR Mission Assurance: Enable reliable and predictable mission support by software and systems, which are resilient to adversary actions

Autonomy & Counter-Autonomy: Develop evidence that indicates the trustworthiness, dependencies, & vulnerabilities of autonomous systems

Human-Machine Interactions: Invent, assess, improve comprehensible, safe, and trustworthy technologies for humans to use and team with machines