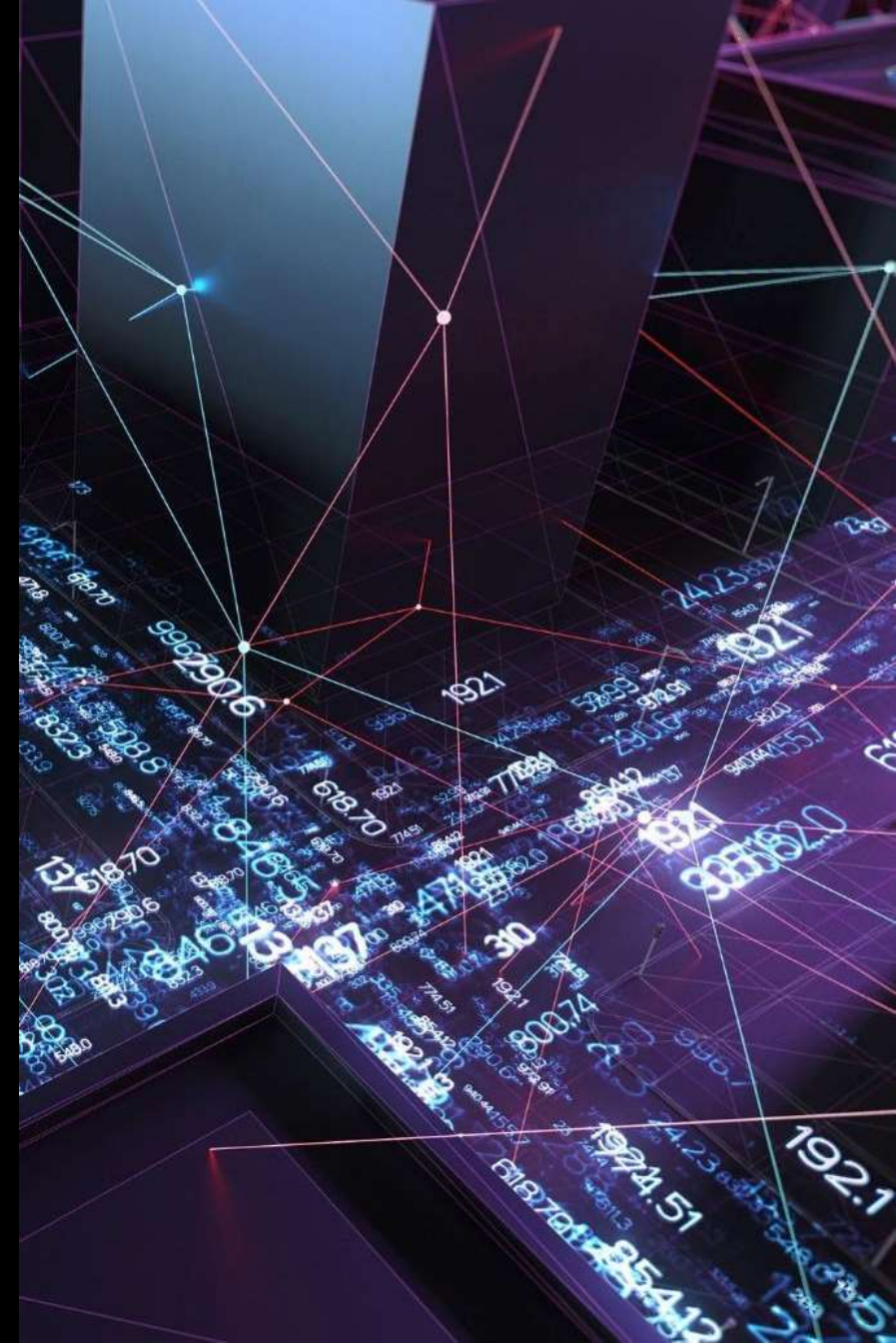


Carnegie Mellon University Software Engineering Institute (SEI) Overview

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

“The FFRDC is required to conduct its business in a manner befitting its special relationship with the government, to operate in the public interest with objectivity and independence, to be free from organizational conflicts of interest, and to have full disclosure of its affairs to the sponsoring agency.”

Federal Acquisition Regulation, 35.017:
“Federally Funded Research and Development Centers”

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

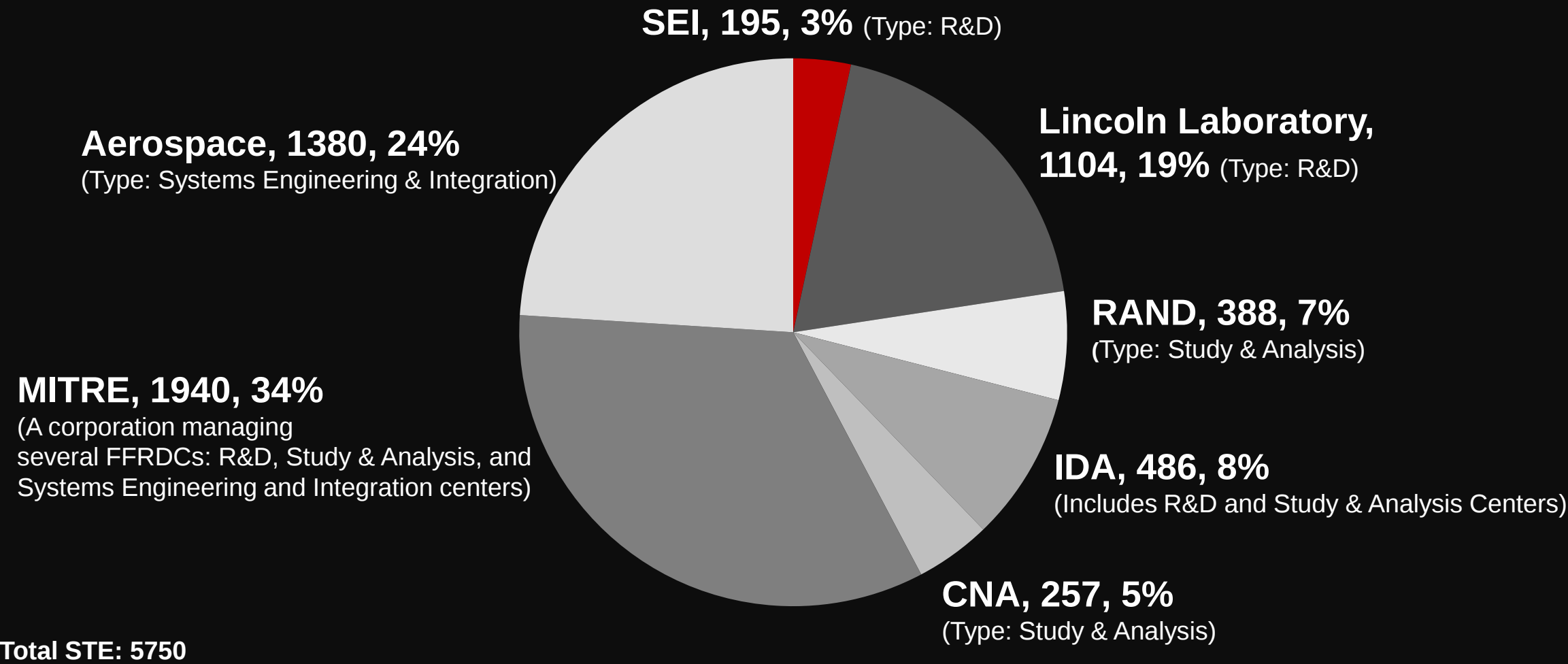
Analyze technical questions with a high degree of objectivity

Three activity types:

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



DoD FFRDCs: Initial FY17 STE Allocations



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



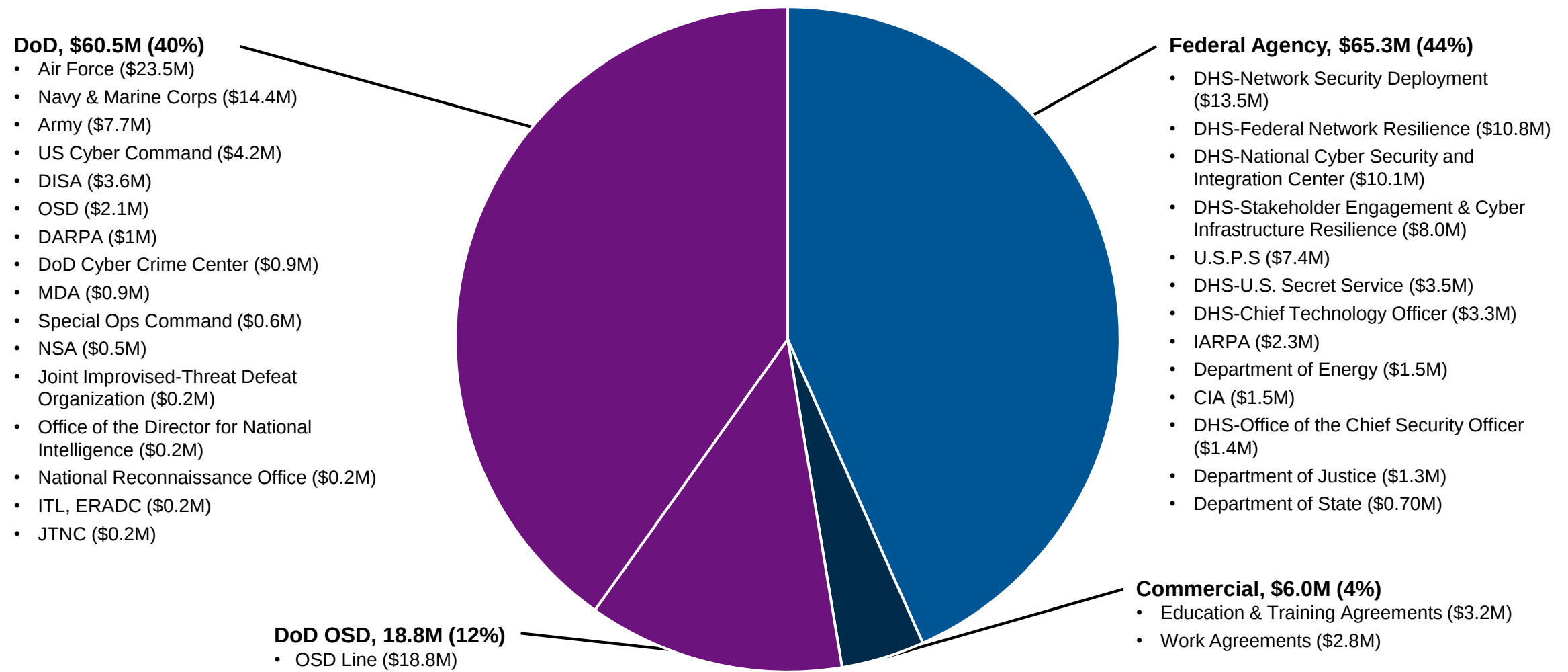
Major government customers

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

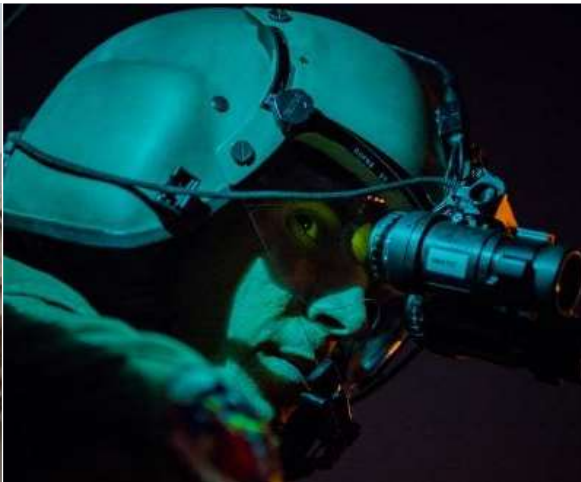
Researchers, developers, users, and acquirers—government, commercial, and academic

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

Our FY17 Work Program Funding Projection (\$150.6M)



Software is Responsible for Greater System Functionality and Desired Qualities



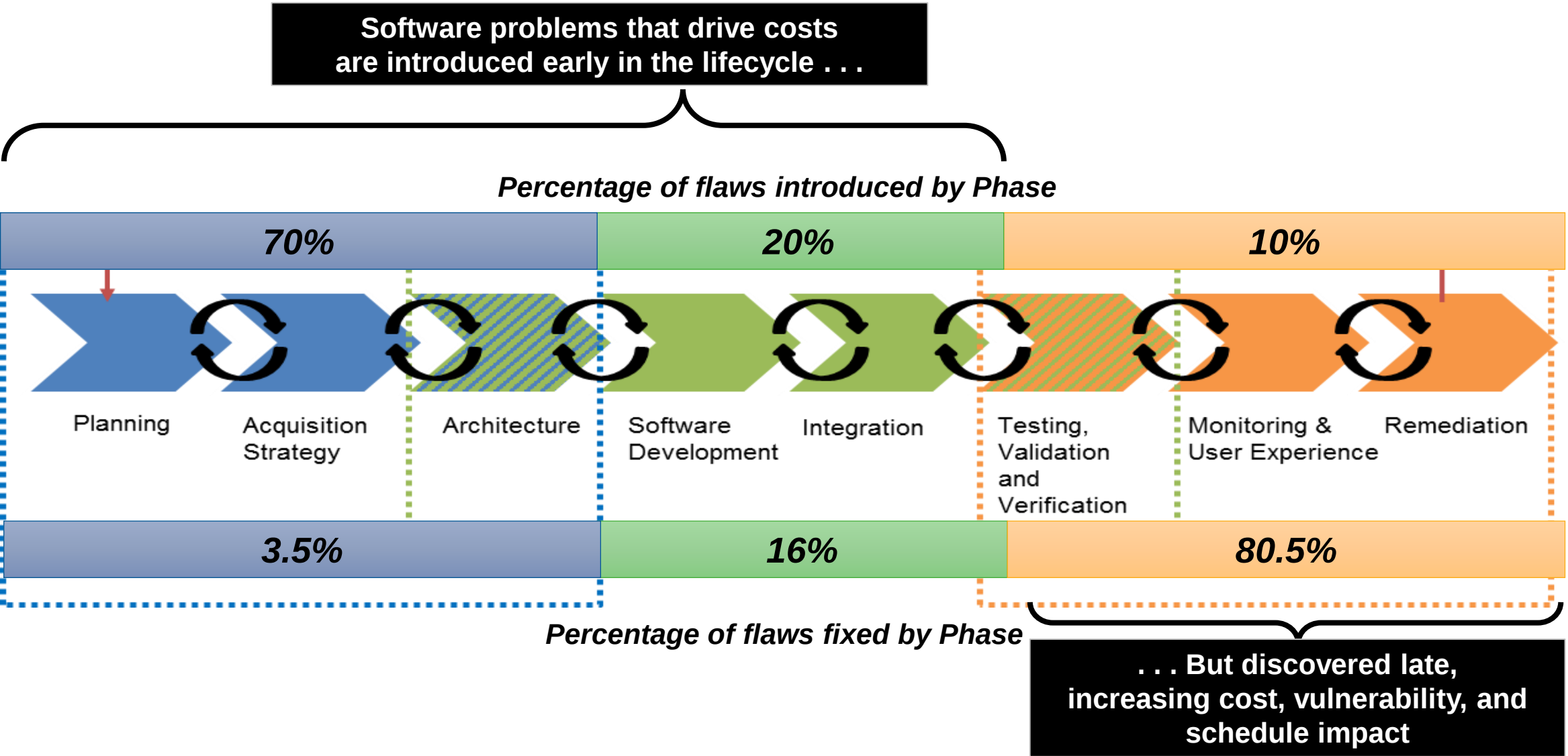
Software can offer

- 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...

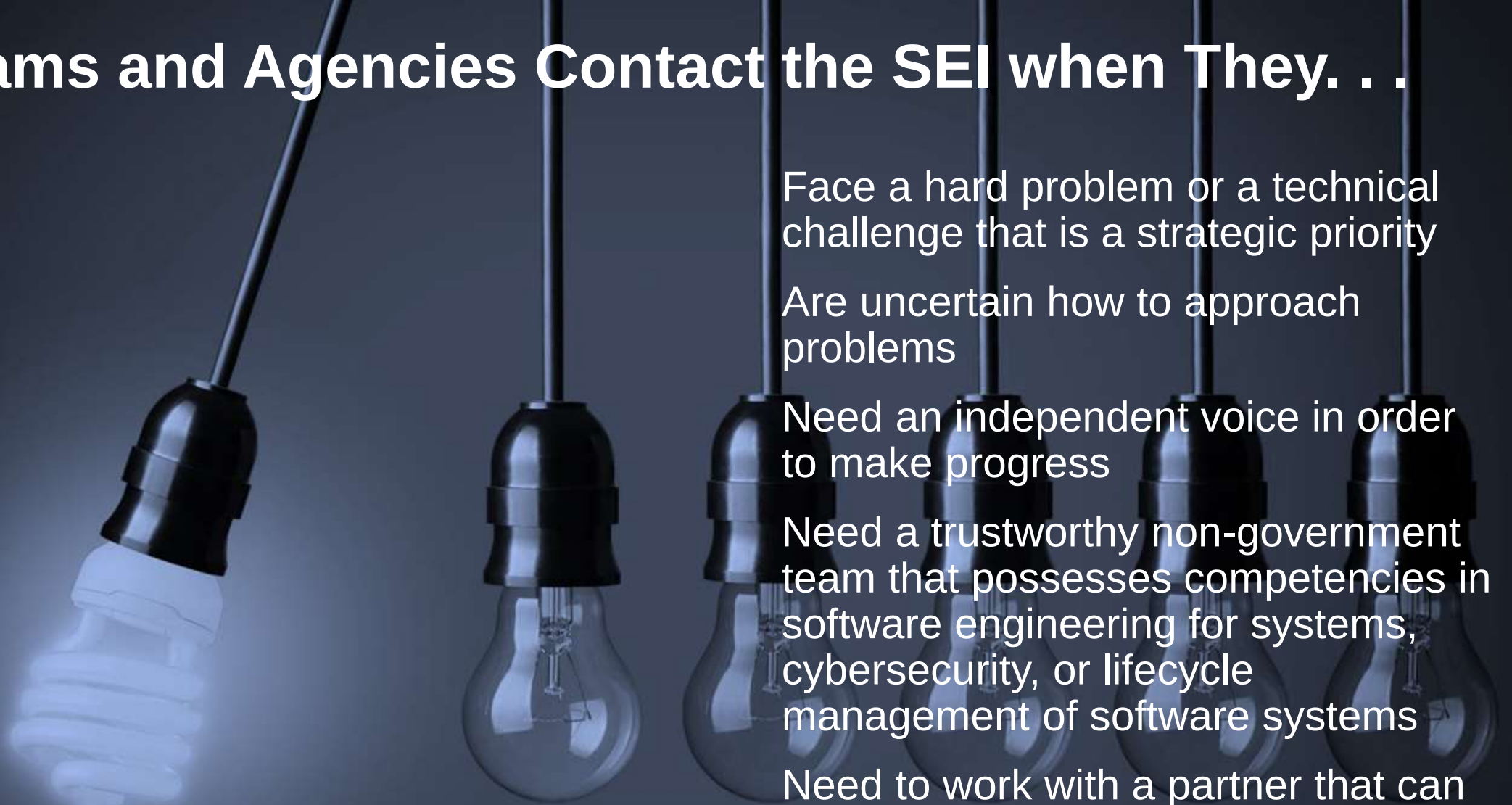
Face a hard problem or a technical challenge that is a strategic priority

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

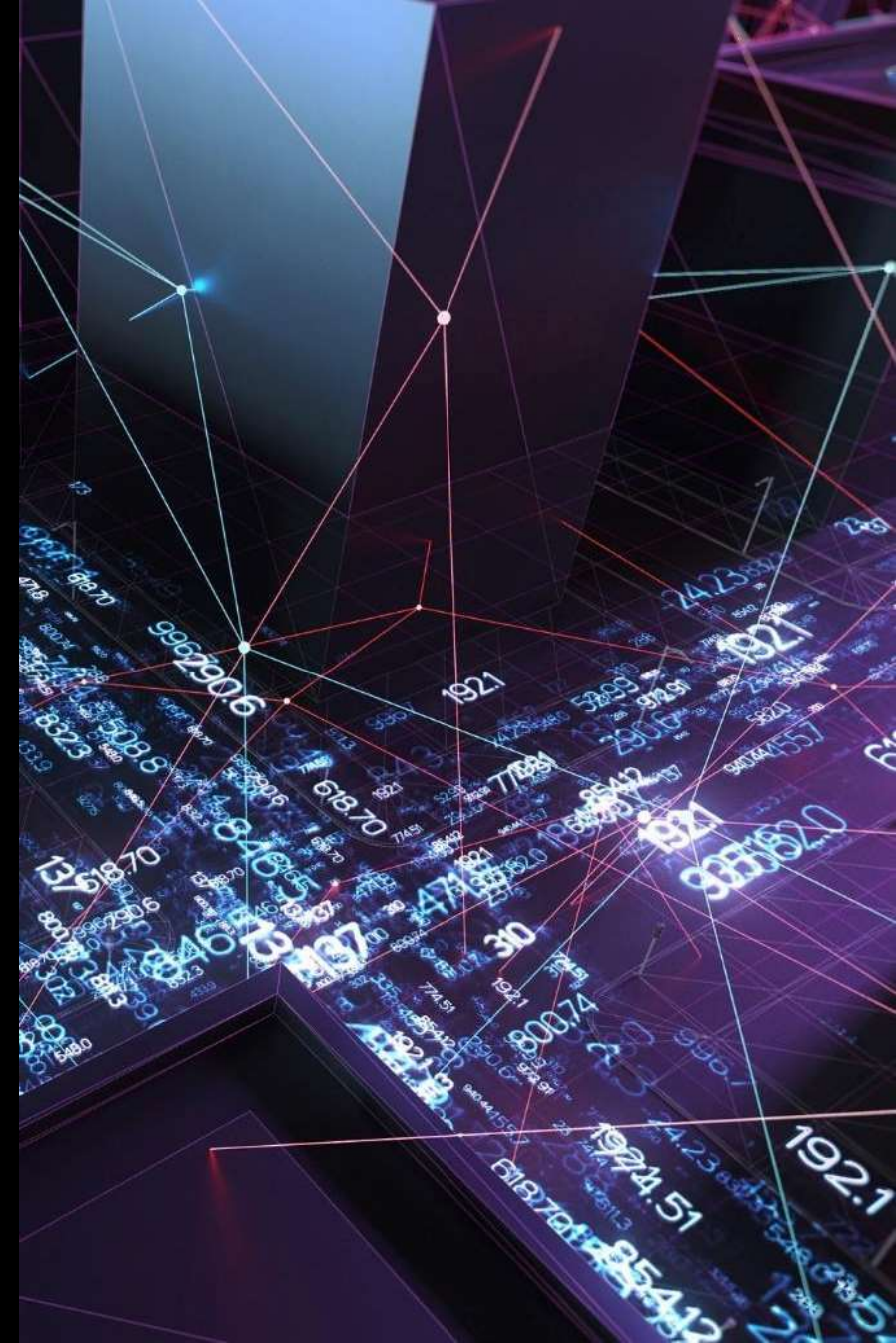
Harry Kaye

Deputy CFO



Software Engineering Institute

Carnegie Mellon University



© 2017 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

SEI Maintains Offices in Six U.S. Cities



SEI Based in Pittsburgh – Four Locations

5th Avenue Building



Collaborative
Innovation Center



Bakery Square



Rand Building



SEI Presence in Arlington, VA



Operating Locations

Leasing small office space in

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

On customer site – Randolph Air Force Base

- San Antonio, TX



Questions ?



Copyright 2017 Carnegie Mellon University. All Rights Reserved.

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

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

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

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

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 use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

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

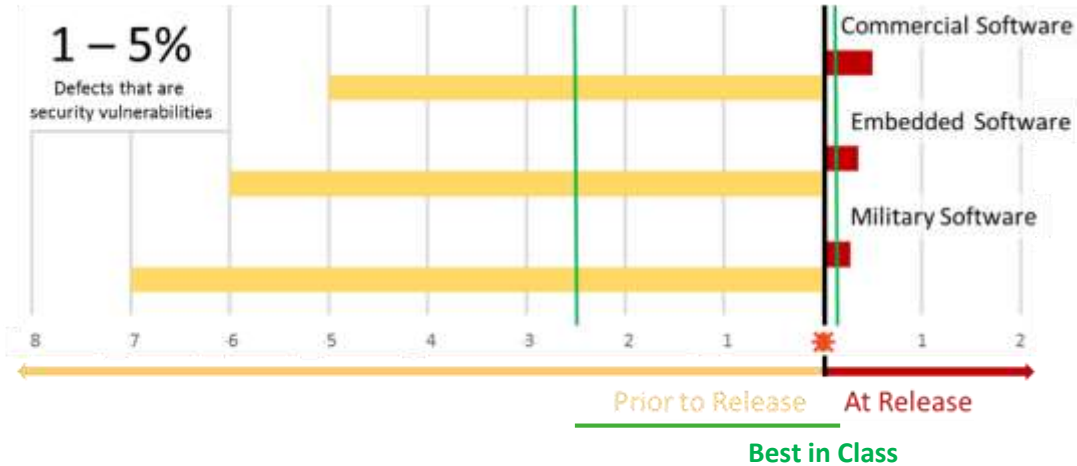
DM17-0565

Backup slides



Software Vulnerabilities put Missions at Risk

Latent Vulnerabilities

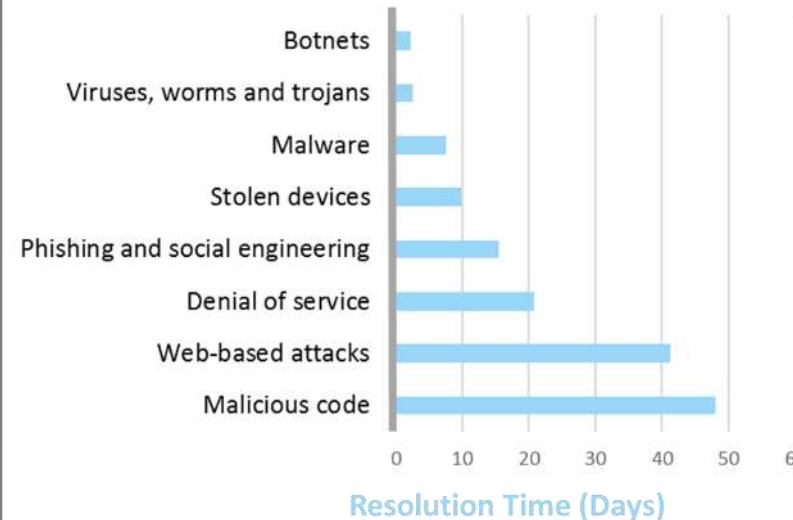


A 10M LOC Weapons Platform written in C will be delivered with 280 – 1,400 exploitable vulnerabilities

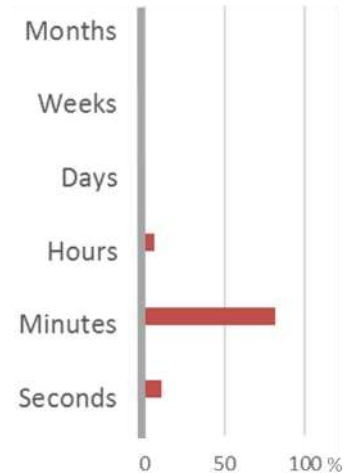
- 1 year after operation, 55% of these vulnerabilities will remain
- In sustainment, new vulnerabilities will be introduced

Cyber Operations Response Lags

US Incident Resolution Averages



Time to Compromise



< 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

Quality Data: Capers Jones, NamCook Analytics, 2012

Vulnerability Data: SEI, Predicting Cybersecurity Using Quality Data, 2015 IEEE International Symposium on Technologies for Homeland Security

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

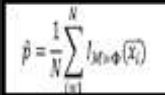
Enhance confidence in the systems engineering lifecycle with evidence-based methods and tools

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



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