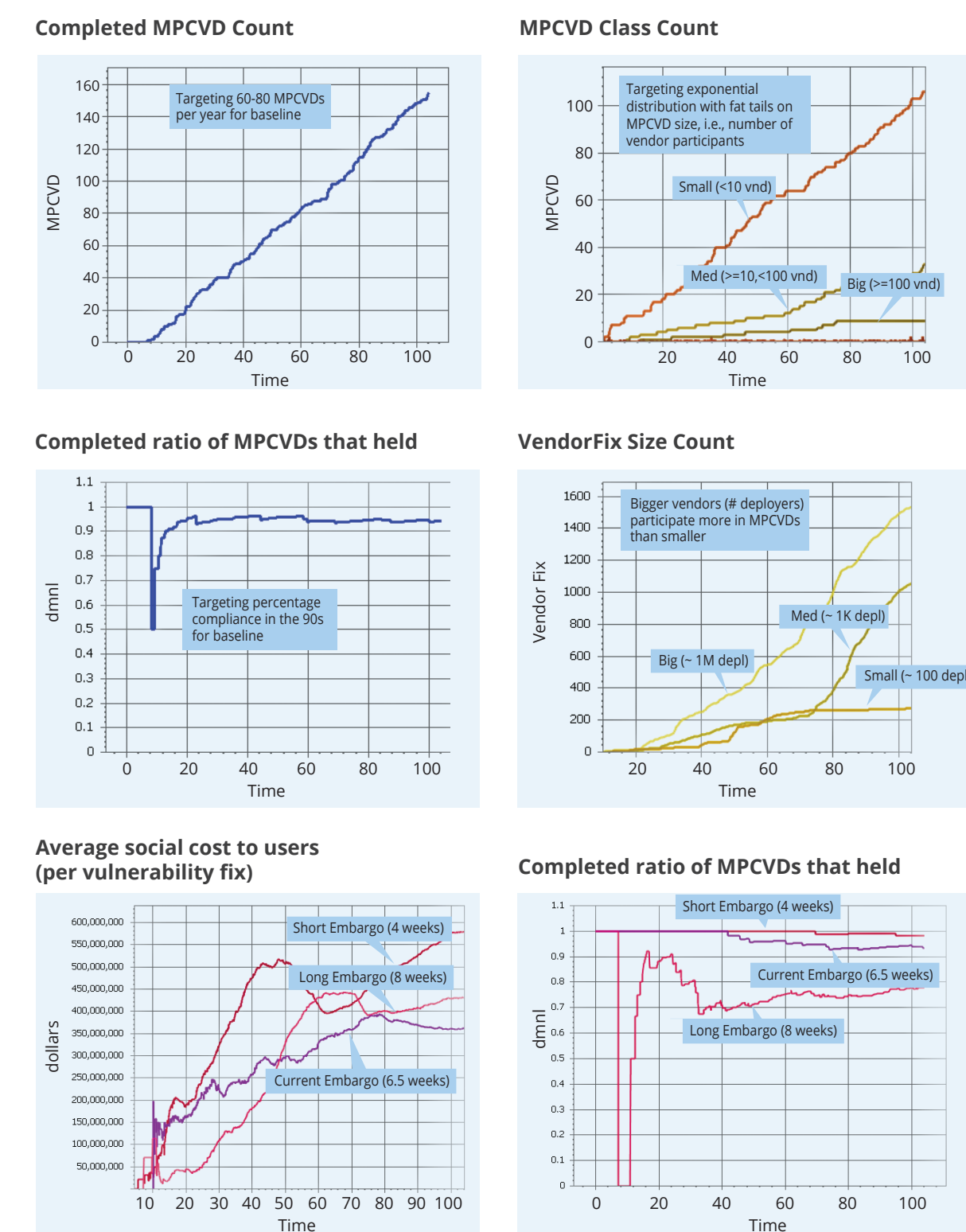


Modeling the Operations of the Vulnerability Ecosystem

Coordinated Vulnerability Disclosure (CVD) is an emerging capability within DoD. But CVD is known to be difficult and prone to controversy when multiple vendors are involved, as in the case of recent vulnerabilities like Meltdown and Spectre. In this LENS project we modeled the factors affecting cooperation in the multiparty CVD process.

Calibration Target Ranges for Baseline

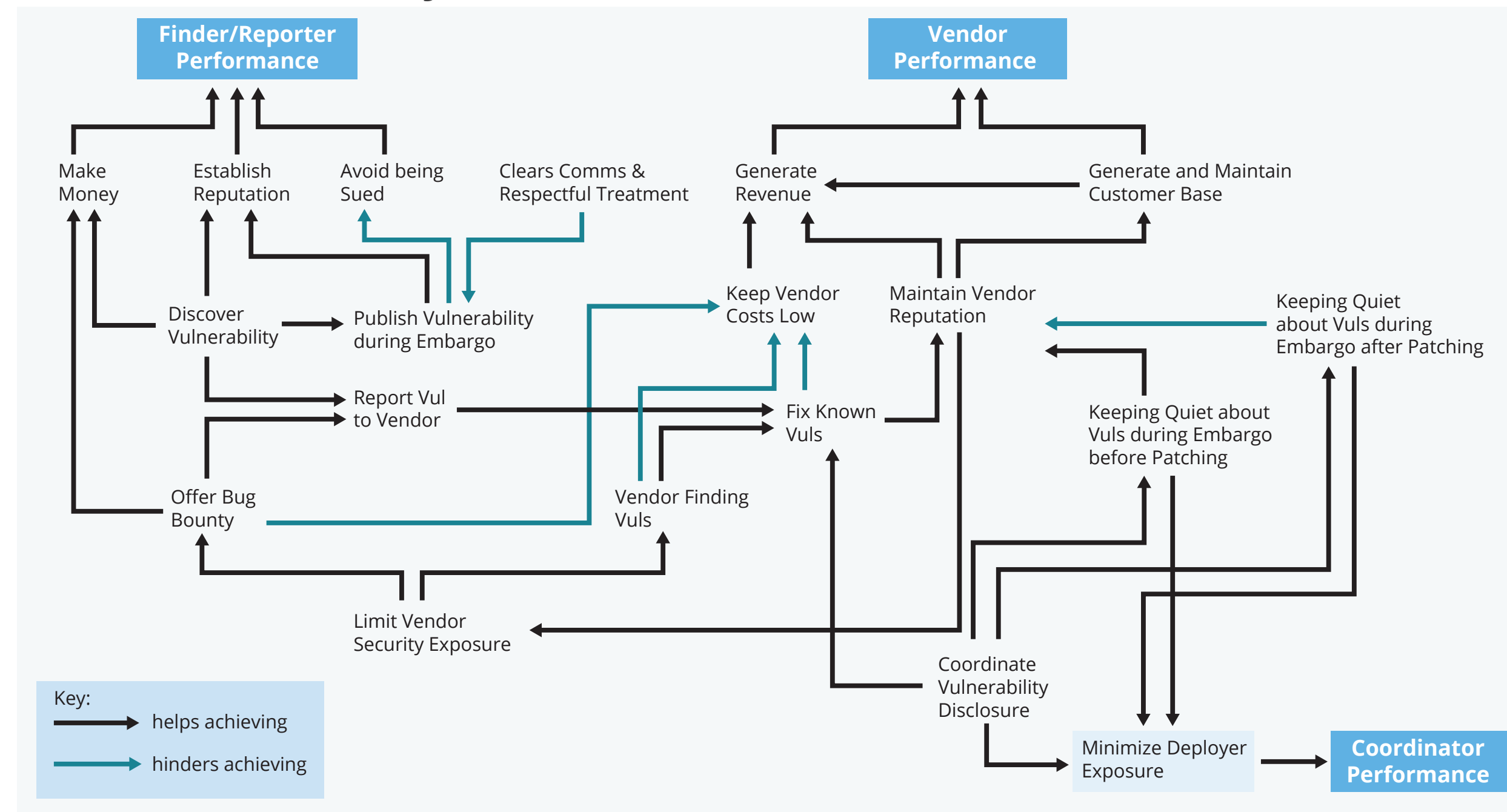


Current embargo (set to about 45 days) to be the lowest cost option per vulnerability fix.

While the short embargo ensures more MPCVDs hold through the embargo period, as seen in the chart on the left, they are the most costly to users. The current embargo period is a good middle ground to reduce cost to users.

Conclusion: Adjusting the embargo period to increase the likelihood that patches can be developed JUST in time appears to be a good strategy for reducing cost.

Drivers of CVD Player Behaviors



Ventury: A Hybrid Modeling Toolset

Ventury is being developed by Ventana Systems, Inc.

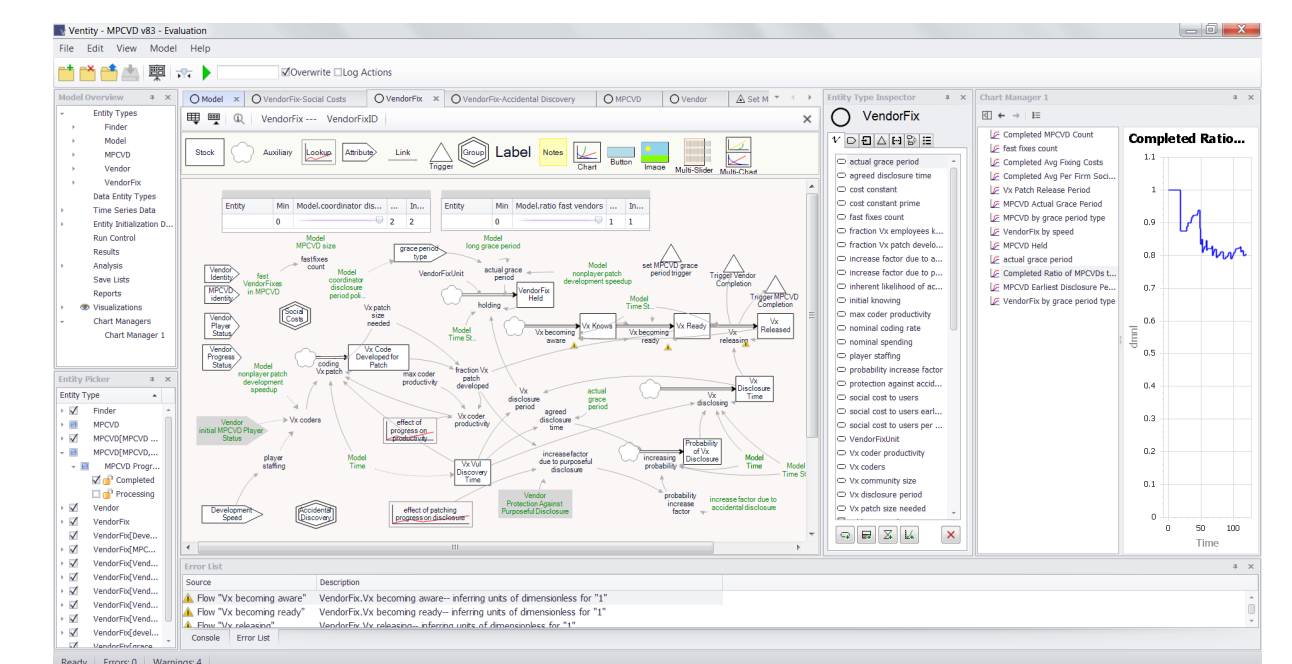
- Modeling and simulation environment supporting two types of modeling
- Agent-based modeling
- System dynamics modeling
- Supports modular construction of socio-technical models for scalable development by independent teams

Used to Model the Multi-Party Coordinated Vulnerability Disclosure (MPCVD) Problem

- Finders, vendors, and MPCVDs are agents
- Simulation runs many MPCVDs over two years to assess management strategies and policies for the coordinator to try out
- Current model under development has been calibrated along several dimensions

- Adjustable model parameters include the number of finders and vendors, size distribution of the MPCVDs and vendors, embargo duration, likelihood of accidental and purposeful disclosure
- Social cost measure includes likelihood of vul exploitation, maximum amount of damage, hacker vul discovery time, attack rate per deployer, amplification of attack rate after disclosure, user workaround costs over time (adapted from Cavusoglu et al., 2007 [1]).

[1] Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2007). Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge. IEEE Transactions on Software Engineering, 33(3), 171-185.

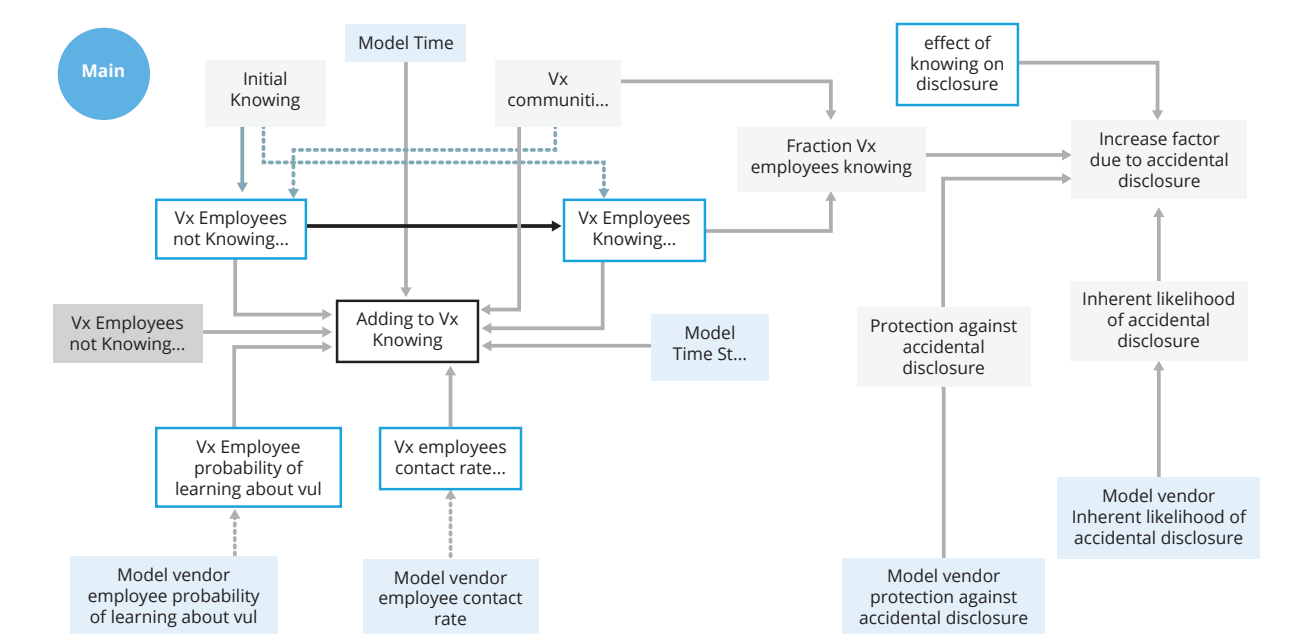


The Ventury Interface

Initial Observations from Non-Validated Model

- The longer after patch development that embargo goes, the greater the chance of renegeing
- The more vendors participating in MPCVDs the more early disclosures that occur
- The sooner that patches are distributed the lower the social cost to deployers, whether patch distributed (and vul disclosed) before or after embargo
- Shortening the embargo time leads to lower rates of renegeing, but high rates of no patch after embargo
- Assumption: Faster patching is more costly for all vendors.

Accidental Disclosure Sector



Copyright 2018 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.

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* is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM18-1133