



# Panel: Coordinating vulnerabilities in AI systems

Harold Booth (NIST)

Jonathan Evans (MITRE)

Ian Malloy (IBM)

Lena Pons (Carnegie Mellon University)

Moderator: Jonathan Spring

Thanks to Brian Lindauer, Zach Kurtz, and Frank Stein for their help organizing this panel

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

# Document Markings

Copyright 2019 Carnegie Mellon University.

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

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

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

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](mailto:permission@sei.cmu.edu).

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

DM19-1174

# Vulnerability management basics

## Vulnerability

- a weakness in an information system, including in its system security procedures, internal controls, requirements, design, or implementation, that could be exploited or triggered by a threat source. (NIST docs define each of these words in turn)

## Vulnerability management includes (per FIRST):

- Vulnerability discovery / research
- Vulnerability report intake
- Vulnerability analysis
- Vulnerability coordination
- Vulnerability disclosure
- Vulnerability response

# Vulnerability management basics II

## CVSS

- “The Common Vulnerability Scoring System provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its [technical] severity.”  
(FIRST, [https://www.first.org/education/csirt\\_services\\_framework\\_v2.0](https://www.first.org/education/csirt_services_framework_v2.0))

NIST’s National Vulnerability Database (NVD) “performs analysis on CVEs that have been published to the CVE Dictionary. NVD staff are tasked with analysis of CVEs... . This analysis results in association impact metrics (Common Vulnerability Scoring System - CVSS), vulnerability types (Common Weakness Enumeration - CWE), and applicability statements (Common Platform Enumeration - CPE)...” <https://nvd.nist.gov/general>

# Panelists

Harold Booth

Jonathan Evans

Ian Malloy

Lena Pons