DEVELOPING HANDS-ON CYBERSECURITY 'CHALLENGES' TO IMPROVE TRAINING AND ASSESSMENT

Jarrett Booz

Carnegie Mellon University
Software Engineering Institute

[Distribution Statement A] Approved for public release and unlimited distribution.

Copyright 2022 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.

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.

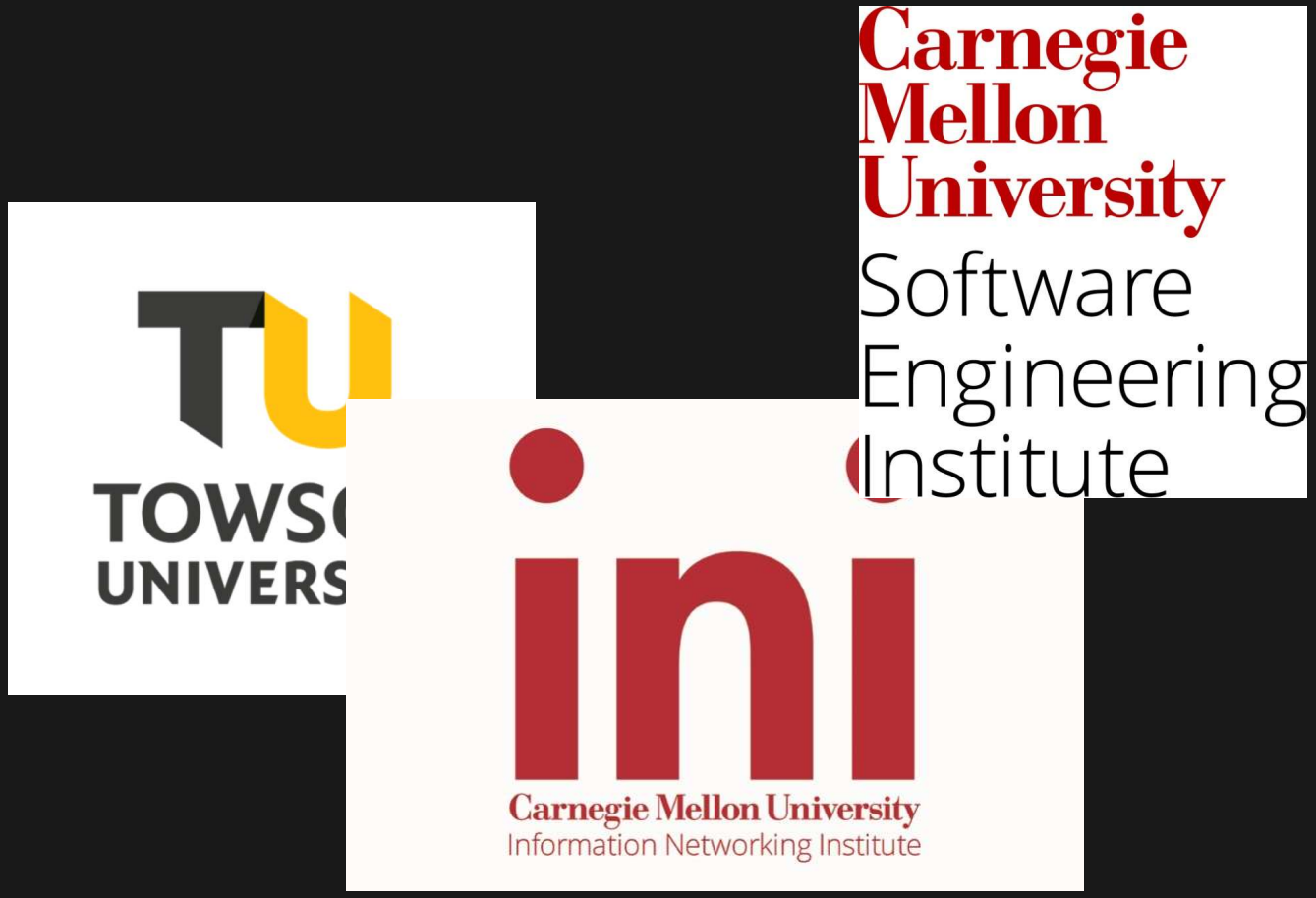
DM22-0998

[Distribution Statement A] Approved for public release and unlimited distribution.

```
$ whoami
```

[Distribution Statement A] Approved for public release and unlimited distribution.

```
$ whoami
jarrett
```



[Distribution Statement A] Approved for public release and unlimited distribution.

WHAT'S THE SEI?

- Founded in **1984** as the only software engineering Federally Funded Research and Development Center (FFRDC)
- Leader in **software engineering**, **cybersecurity** and **artificial intelligence** research
- **~730** employees
- Headquarters in **Pittsburgh, PA**; Other offices near strategic partners in CA, MA, MD and VA

[Distribution Statement A] Approved for public release and unlimited distribution.

CERT Cyber Workforce Development (CWD)

[Distribution Statement A] Approved for public release and unlimited distribution.

CWD DIRECTORATE MISSION

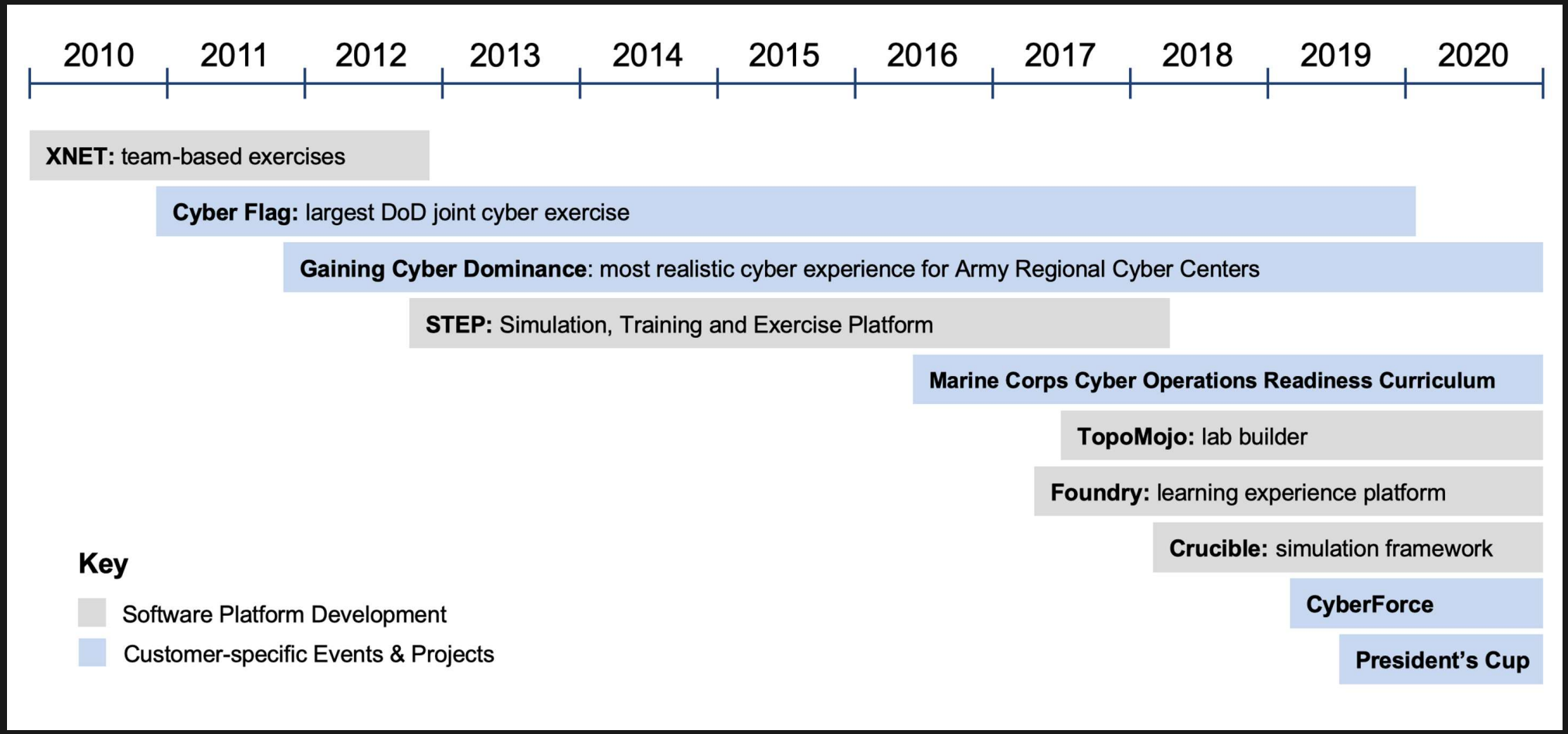
*Provide force-multiplying solutions to rapidly grow and strengthen the nation's cybersecurity workforce—addressing the problems of **time**, **scale**, and **cost**.*

Find the **gap areas** that industry has not addressed *(yet)*.

[Distribution Statement A] Approved for public release and unlimited distribution.

What does that look like?

[Distribution Statement A] Approved for public release and unlimited distribution.



[Distribution Statement A] Approved for public release and unlimited distribution.

How **big** is the problem?

[Distribution Statement A] Approved for public release and unlimited distribution.

769,736

[Distribution Statement A] Approved for public release and unlimited distribution.

769,736

U.S. CYBERSECURITY JOB OPENINGS

Source: Cyberseek Interactive Map, October 2022

[Distribution Statement A] Approved for public release and unlimited distribution.

[Distribution Statement A] Approved for public release and unlimited distribution.

How do we address this?

[Distribution Statement A] Approved for public release and unlimited distribution.

How do we address this?

- Attracting people is half the battle
- Hands-on training and realistic experiences
- Maintain engagement while learning

https://www.dhs.gov/science-and-technology/cybersecurity-competitions

[Distribution Statement A] Approved for public release and unlimited distribution.

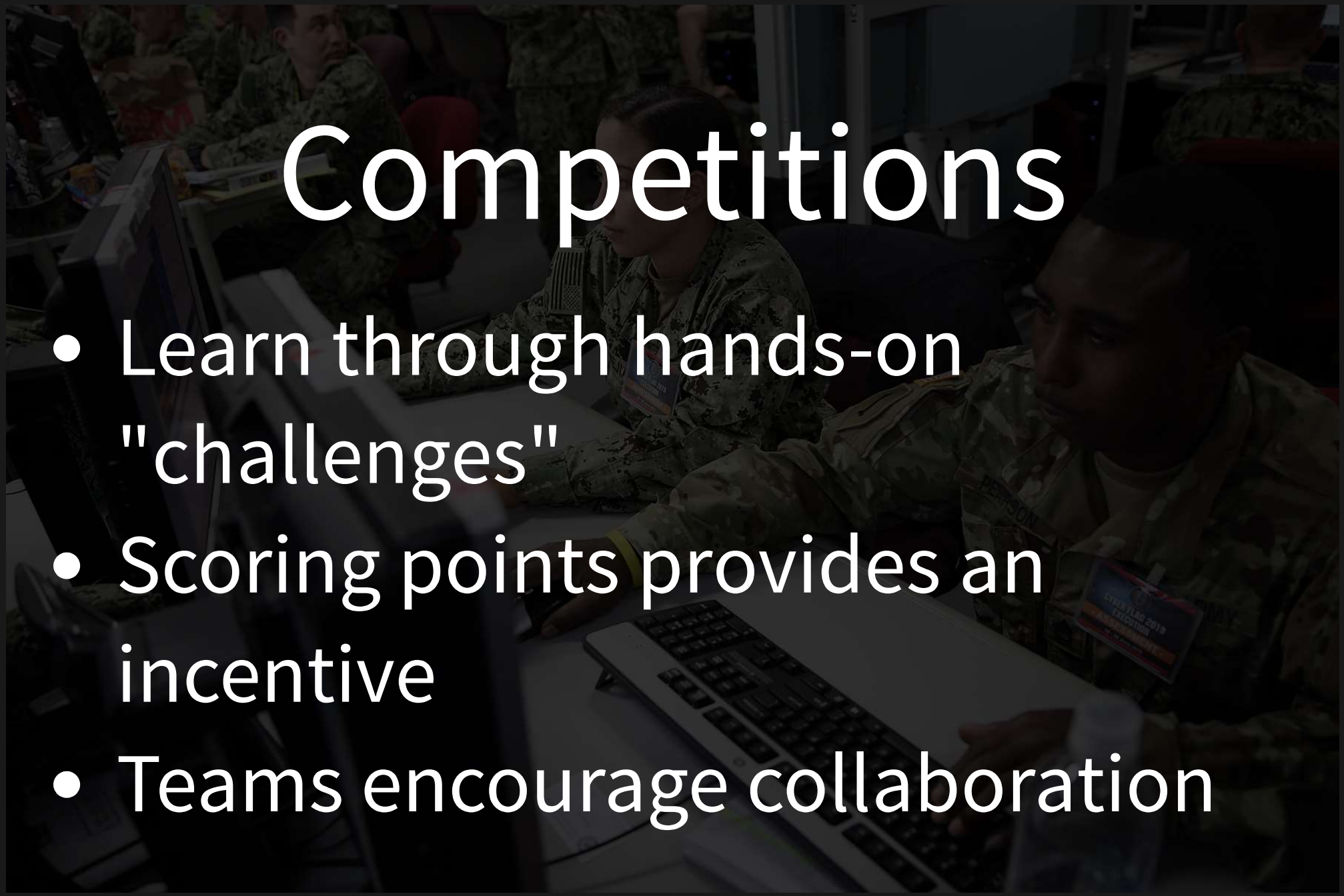
[Distribution Statement A] Approved for public release and unlimited distribution.

[Distribution Statement A] Approved for public release and unlimited distribution.

Competitions

- Learn through hands-on "challenges"

[Distribution Statement A] Approved for public release and unlimited distribution.



Competitions

- Learn through hands-on "challenges"
- Scoring points provides an incentive
- Teams encourage collaboration

[Distribution Statement A] Approved for public release and unlimited distribution.

Our Competition Experience

[Distribution Statement A] Approved for public release and unlimited distribution.

[Distribution Statement A] Approved for public release and unlimited distribution.

- Established in 2019 by E.O. 13870
- 4th year of yearly competition
- 1500 federal gov participants yearly

[Distribution Statement A] Approved for public release and unlimited distribution.

[Distribution Statement A] Approved for public release and unlimited distribution.

What is a "Challenge"?

[Distribution Statement A] Approved for public release and unlimited distribution.

What is a "Challenge"?

- Hands-on labs to test or teach a skill(s)
- Targeted exercises test applicable skills

[Distribution Statement A] Approved for public release and unlimited distribution.

NICE APPLICABLE SKILLS

- NICE Framework publishes gov standard Work Roles, Tasks, Skills, etc.
- Ensure each challenge assesses a NICE Work Role/Task/Skill (e.g., Cyber Defense Analyst)

[Distribution Statement A] Approved for public release and unlimited distribution.

Challenge Planning

[Distribution Statement A] Approved for public release and unlimited distribution.

Challenge Planning

- Challenge Difficulty
- Technical Planning
- Scenario Planning

[Distribution Statement A] Approved for public release and unlimited distribution.

Challenge Development

[Distribution Statement A] Approved for public release and unlimited distribution.

Best Practices

- Testing Applicable Skills
- Required Tools are available/free to use
- Multiple Solution Options
- Clean up after development

[Distribution Statement A] Approved for public release and unlimited distribution.

Challenge Grading

[Distribution Statement A] Approved for public release and unlimited distribution.

Challenge Grading

- Token Discovery
- Question and Answer
- Environment Verification

[Distribution Statement A] Approved for public release and unlimited distribution.

Challenge Variation

- Allows for replay without knowledge of answers
- Discourages answer sharing

[Distribution Statement A] Approved for public release and unlimited distribution.

Solution Guides

- Detailed instructions on a possible solution
- Include explanations for each step

[Distribution Statement A] Approved for public release and unlimited distribution.

Open Source Challenges

- github.com/cisagov/prescup-challenges
- presidentscup.cisa.gov/archive

[Distribution Statement A] Approved for public release and unlimited distribution.

Challenge Development White Paper

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=888592

[Distribution Statement A] Approved for public release and unlimited distribution.

THANKS!

To continue the conversation…

info@sei.cmu.edu

[Distribution Statement A] Approved for public release and unlimited distribution.