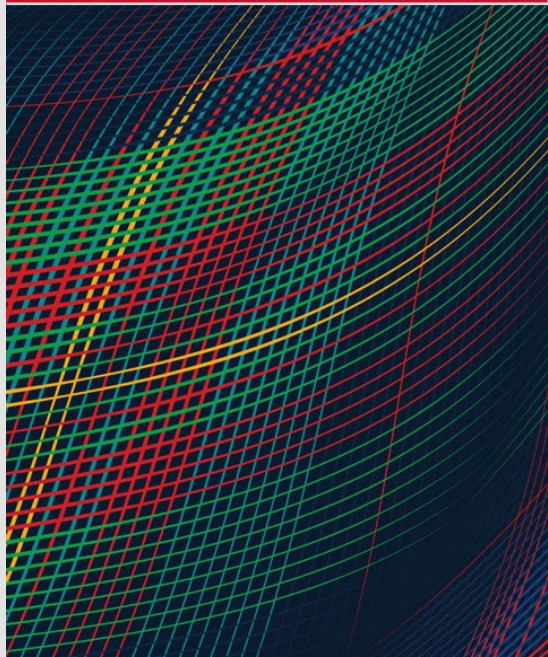
Carnegie Mellon University
Software Engineering Institute



A Peek Behind the Curtain: Securely Maintaining a Development Platform

JUNE 13, 2023

Lyndsi Hughes
David Sweeney

© 2023 Carnegie Mellon University

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

Document Markings

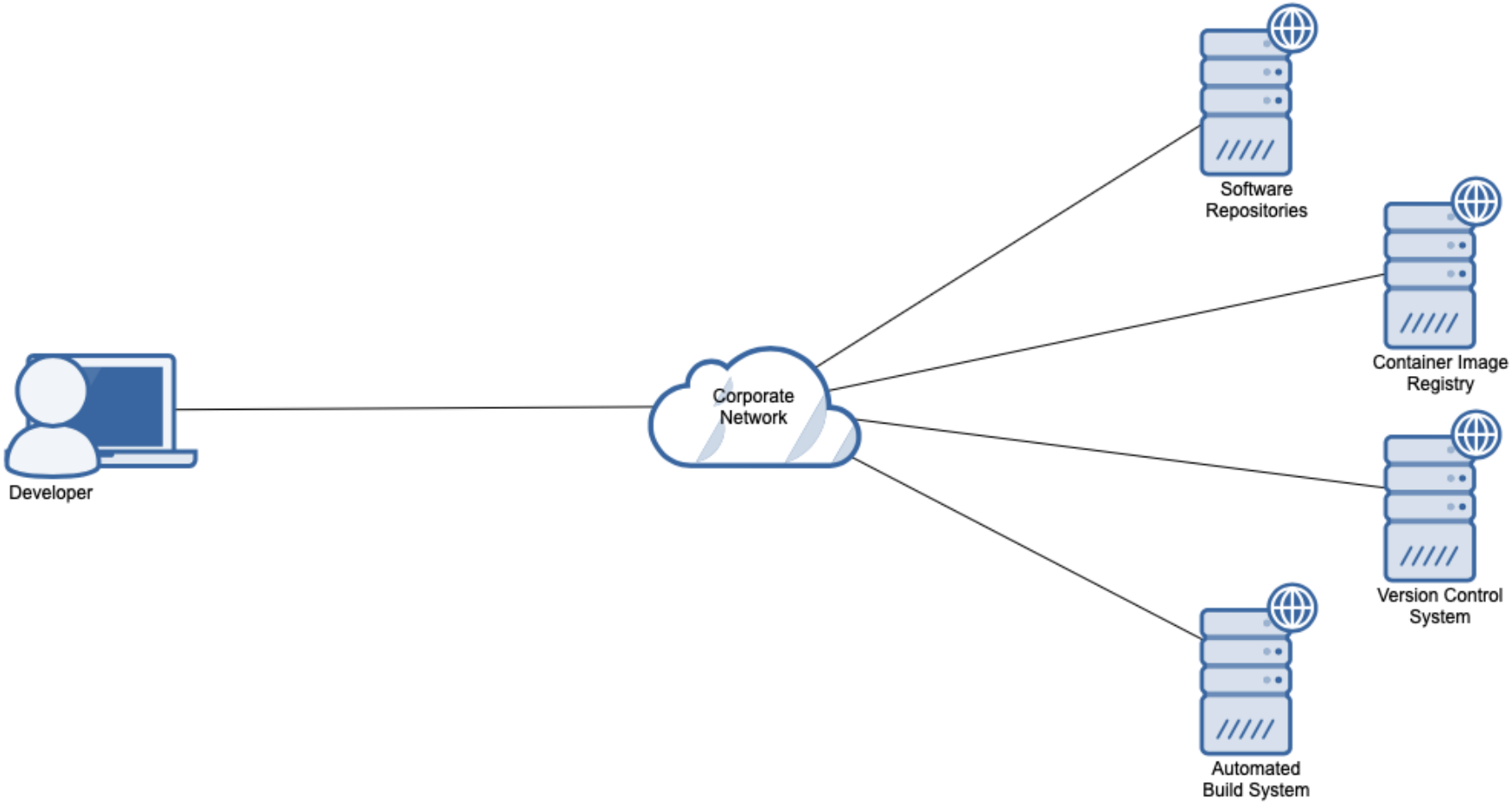
Copyright 2023 Carnegie Mellon University.
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.
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.
DM23-0569

A Peek Behind the Curtain: Securely Maintaining a Development Platform

Developers' Perspectives

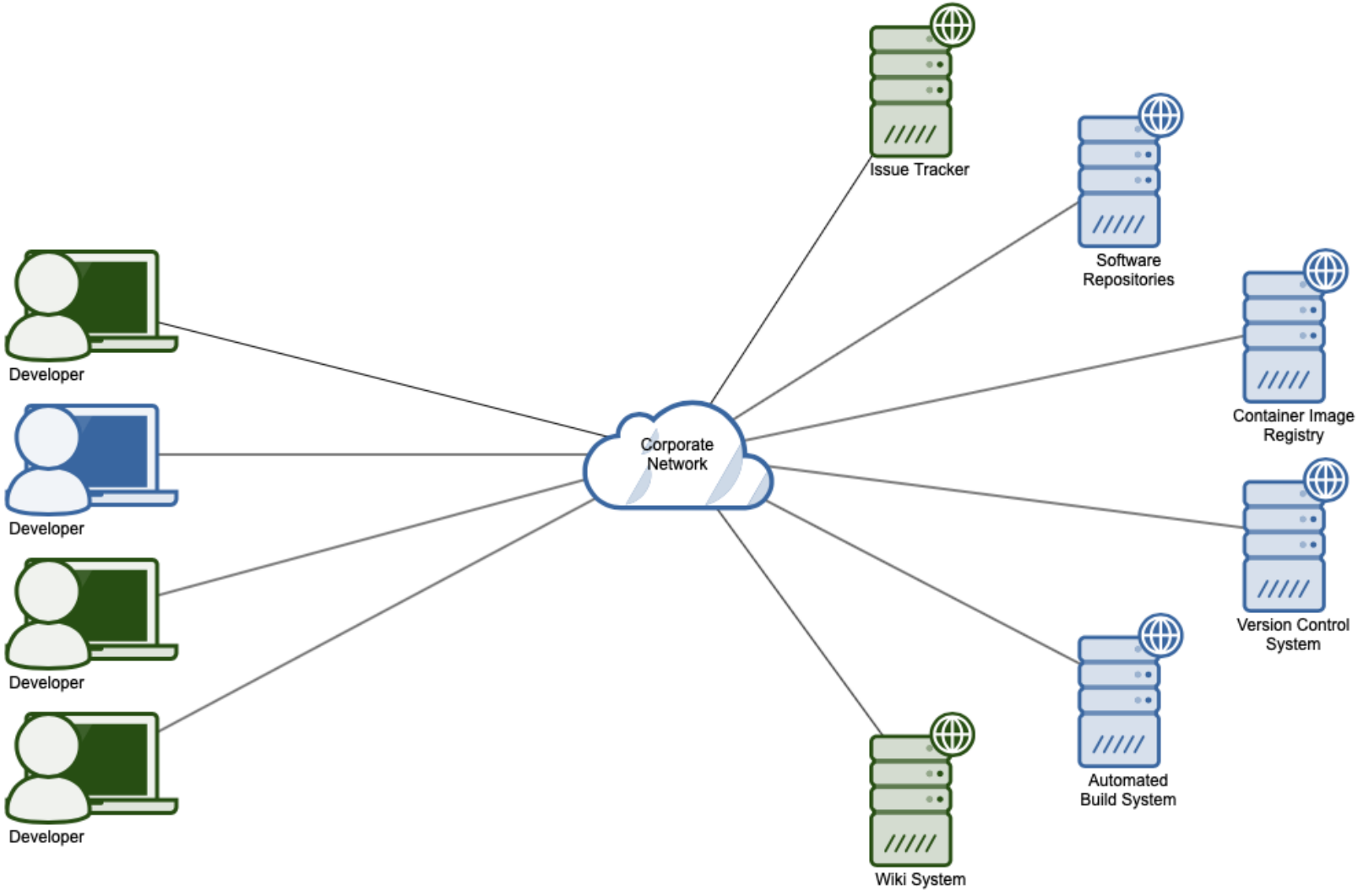
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Carnegie Mellon University
Software Engineering Institute



© 2023 Carnegie Mellon University

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



© 2023 Carnegie Mellon University

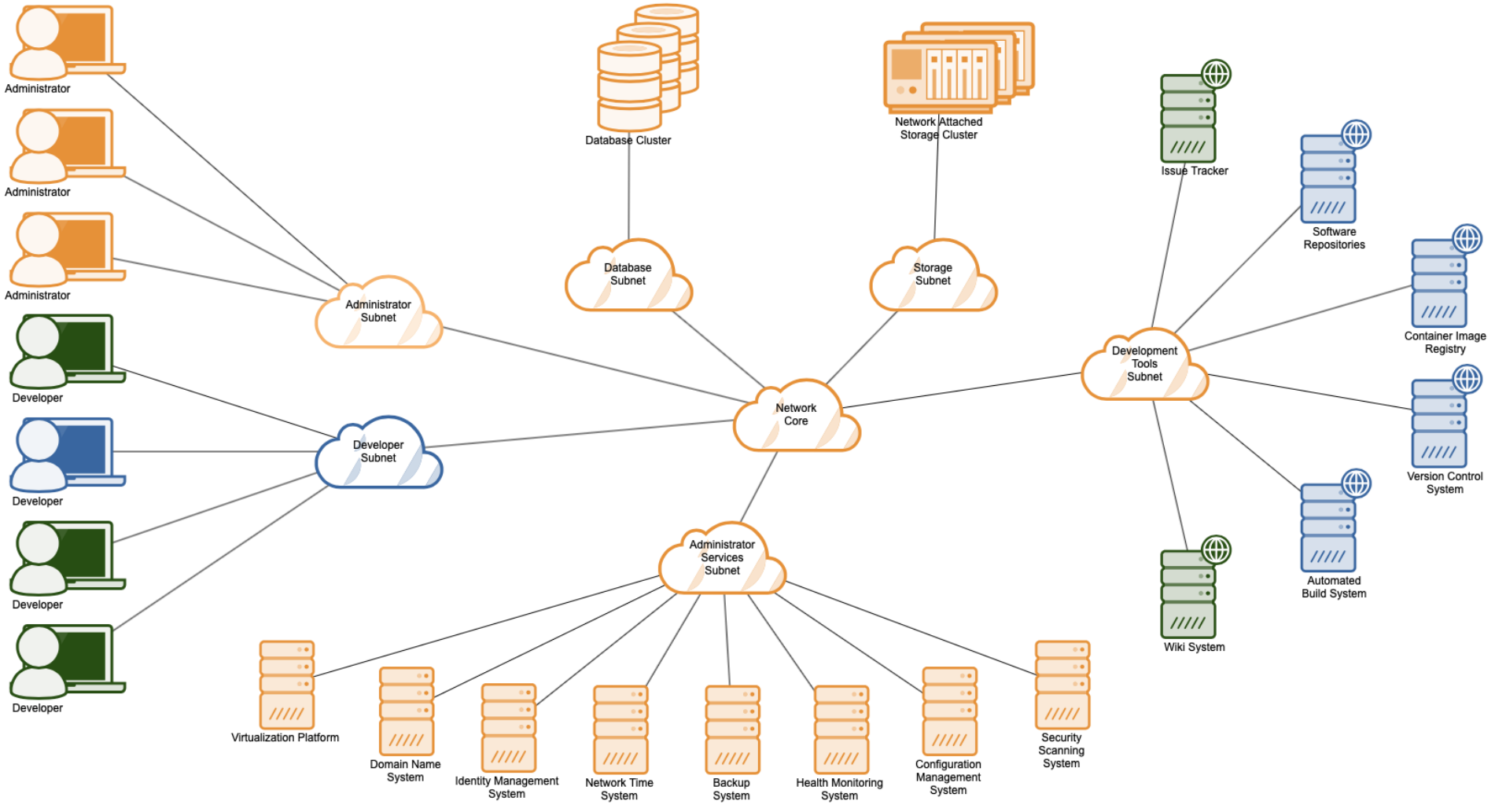
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

A Peek Behind the Curtain: Securely Maintaining a Development Platform

Infrastructure Administrators' Perspectives

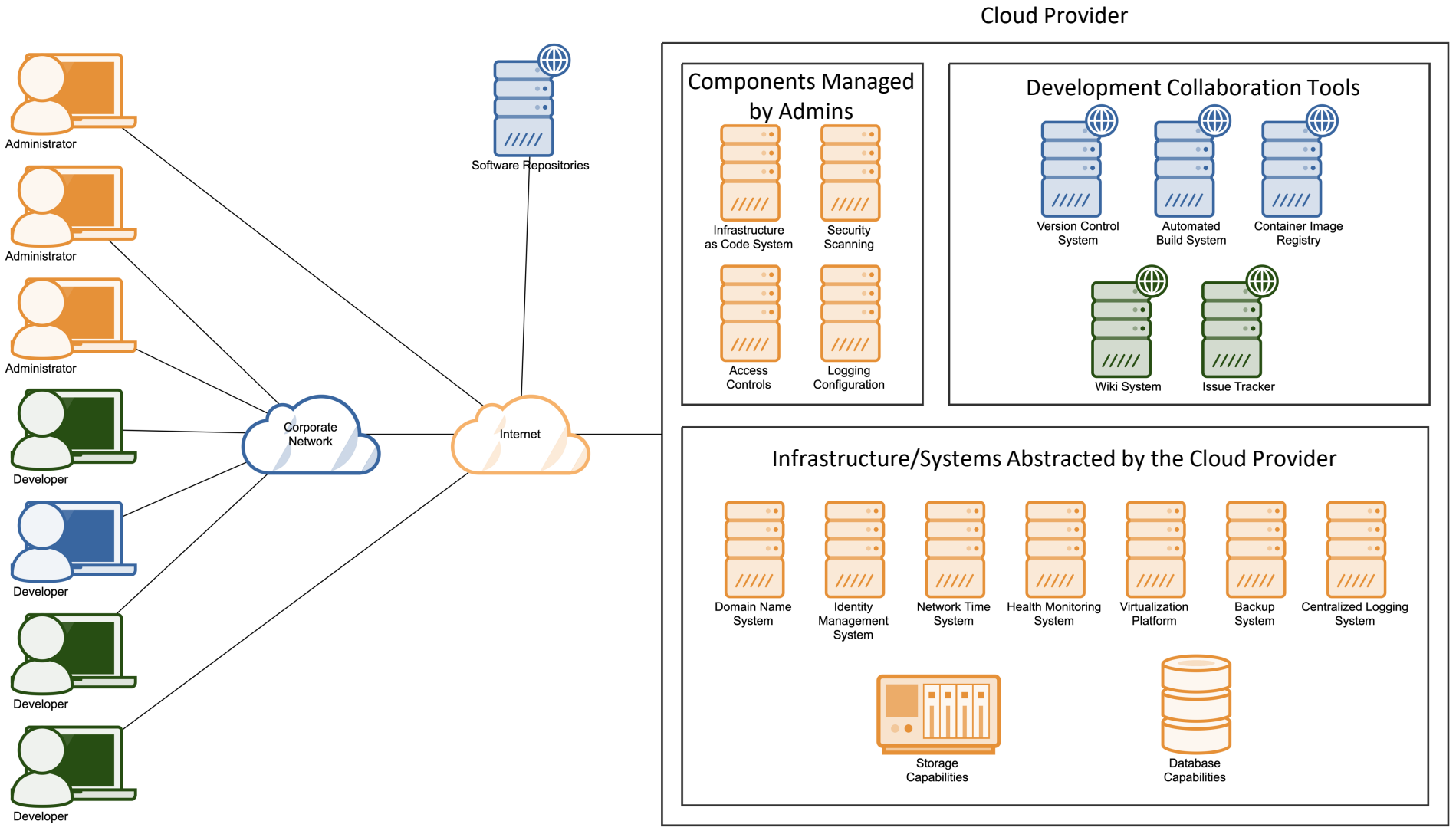
Carnegie Mellon University
Software Engineering Institute

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



© 2023 Carnegie Mellon University

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



© 2023 Carnegie Mellon University

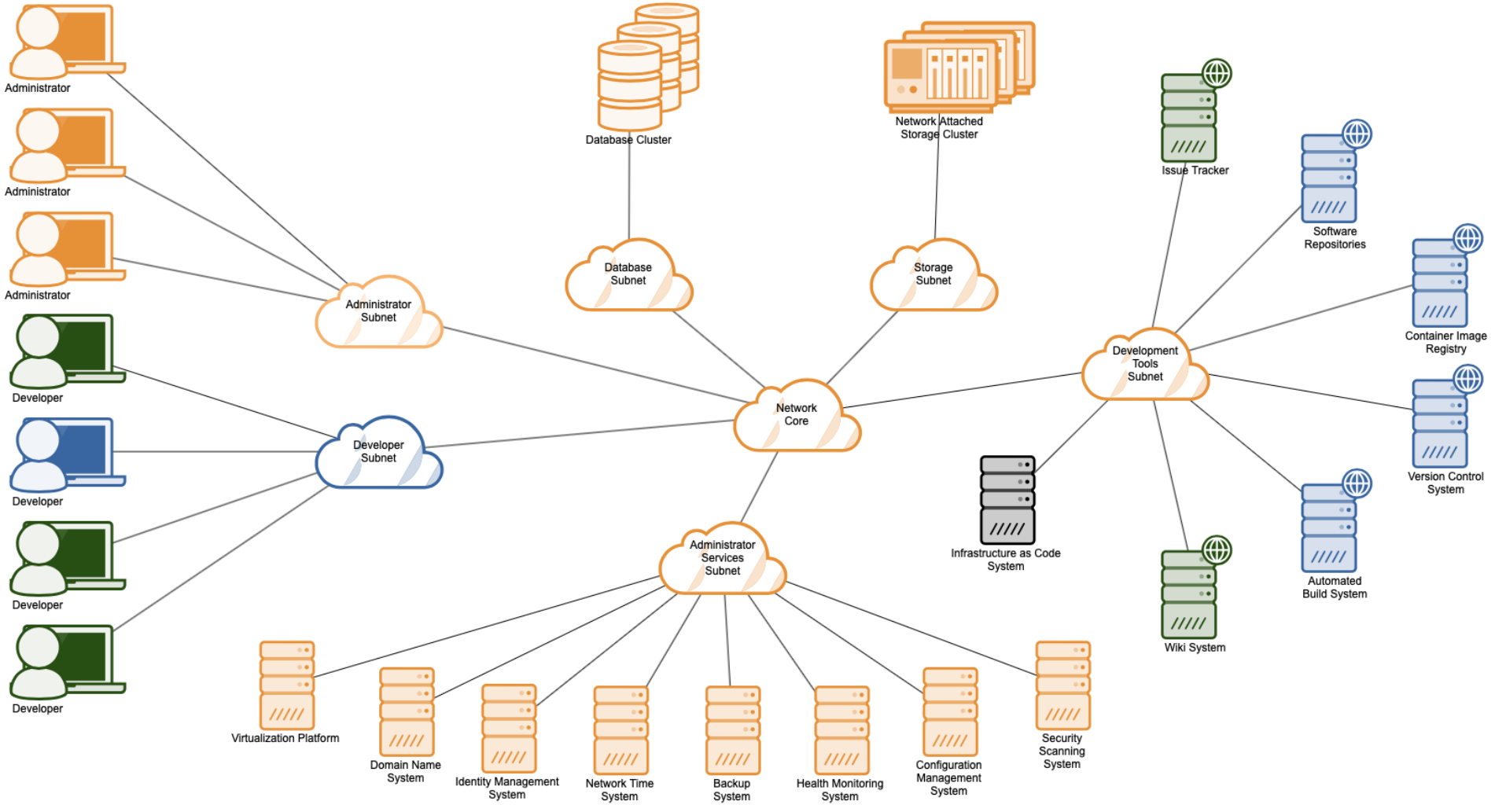
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

A Peek Behind the Curtain: Securely Maintaining a Development Platform

Secure Platform Design

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

Carnegie Mellon University
Software Engineering Institute



© 2023 Carnegie Mellon University

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

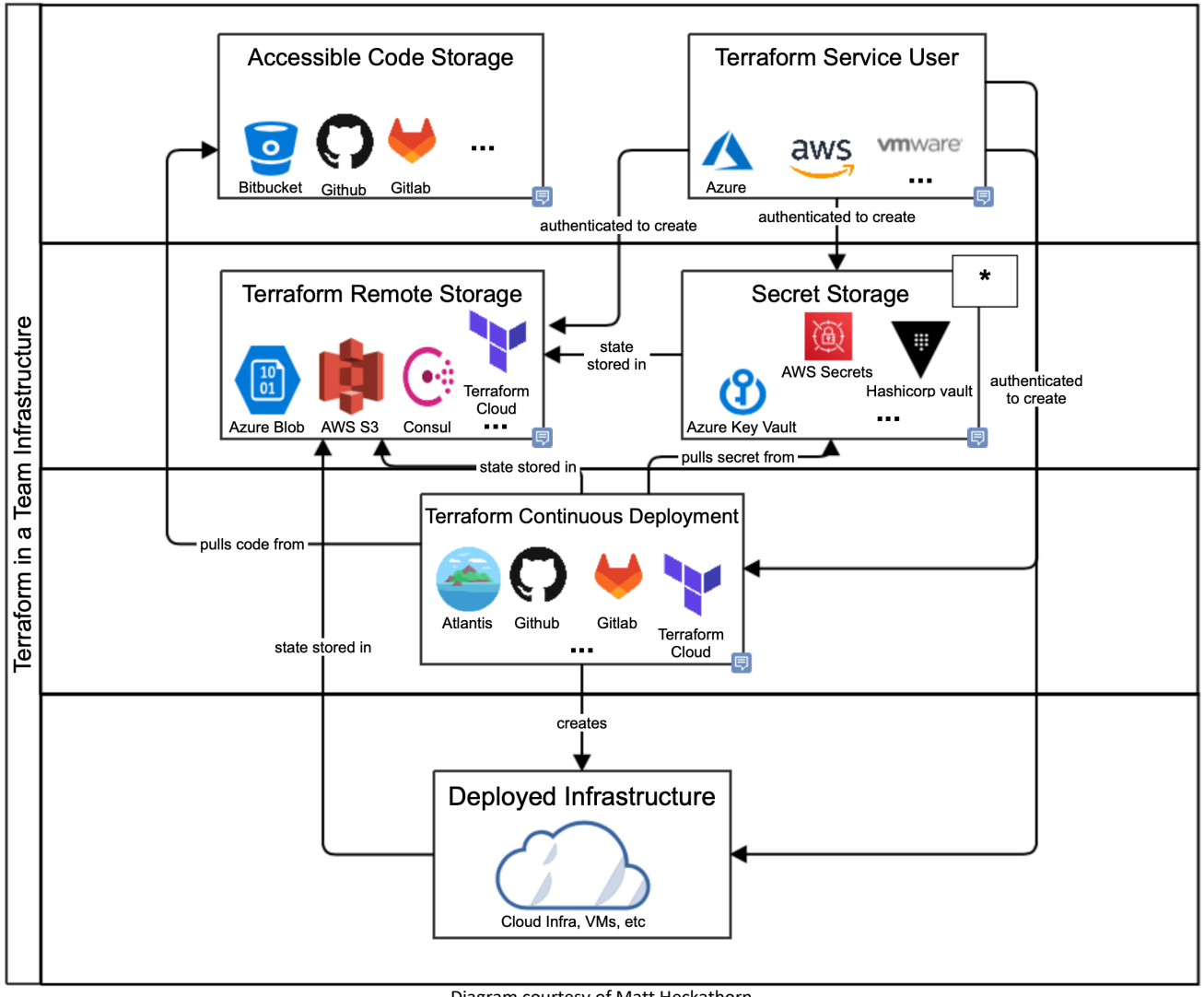


Diagram courtesy of Matt Heckathorn

© 2023 Carnegie Mellon University

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

Secure Component Operation


```
for each component do:
    plan deployment of component
    perform secure initial configuration of component
    write documentation for component

    while component in service:
        patch/update/upgrade component periodically
        scan component for vulnerabilities periodically
        audit component logs periodically
        monitor component health
        maintain and update component documentation

    decommission component
```


© 2023 Carnegie Mellon University

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

Secure Environment Operation

- Understand your sphere of influence
  - what systems exist within your sphere?
  - how do your systems interact with things outside of your sphere?
  - what documents should exist in your library of knowledge?

- Understand the impact of changes within your sphere
  - adding/removing components
  - reconfiguring components
  - adding automation

© 2023 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Contact Us

Lyndsi Hughes
Senior Systems Engineer

David Sweeney
Associate Software Developer

Vanessa Jackson
Senior Engineer

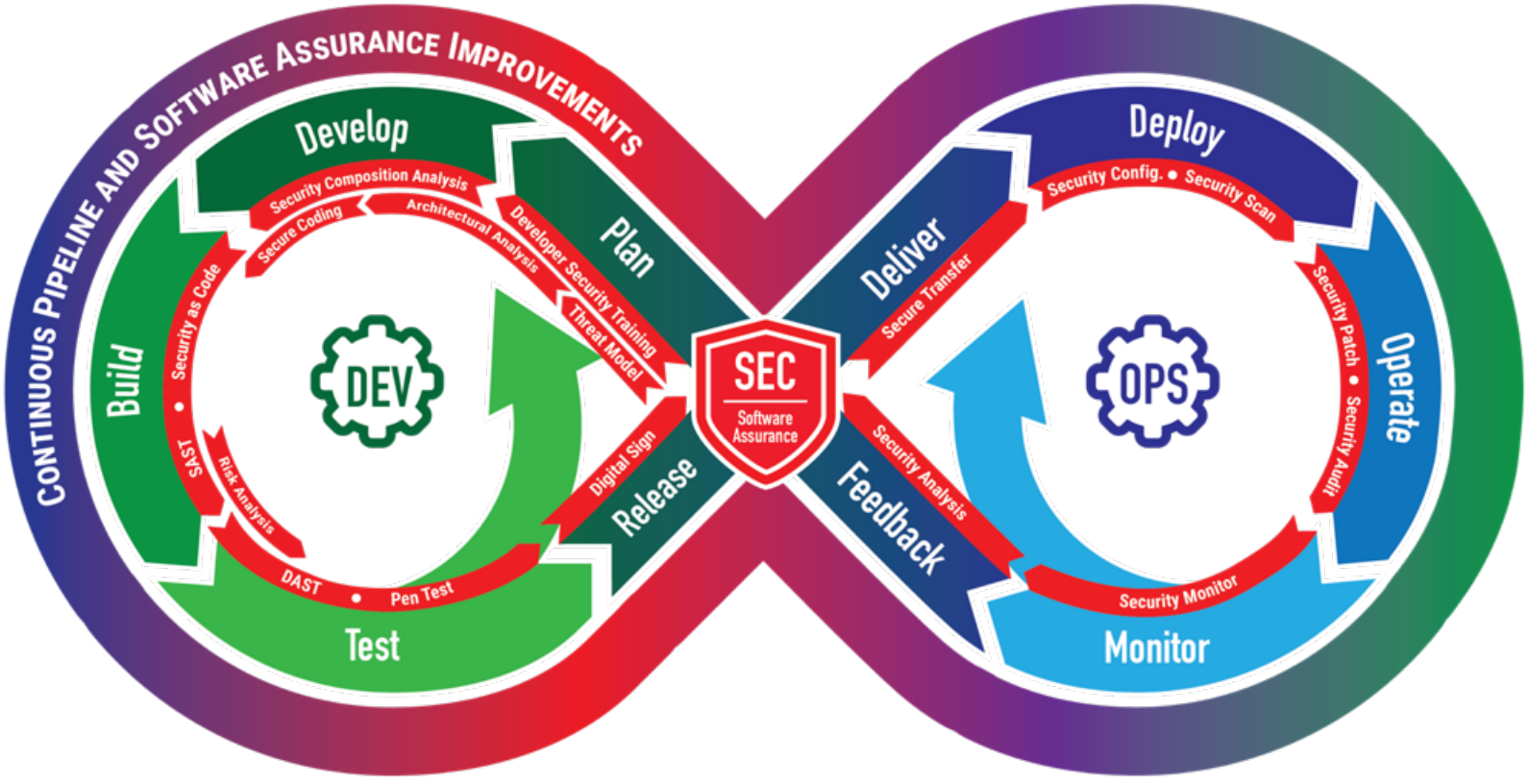
Matt Heckathorn
Integration Engineer

info@sei.cmu.edu

© 2023 Carnegie Mellon University

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

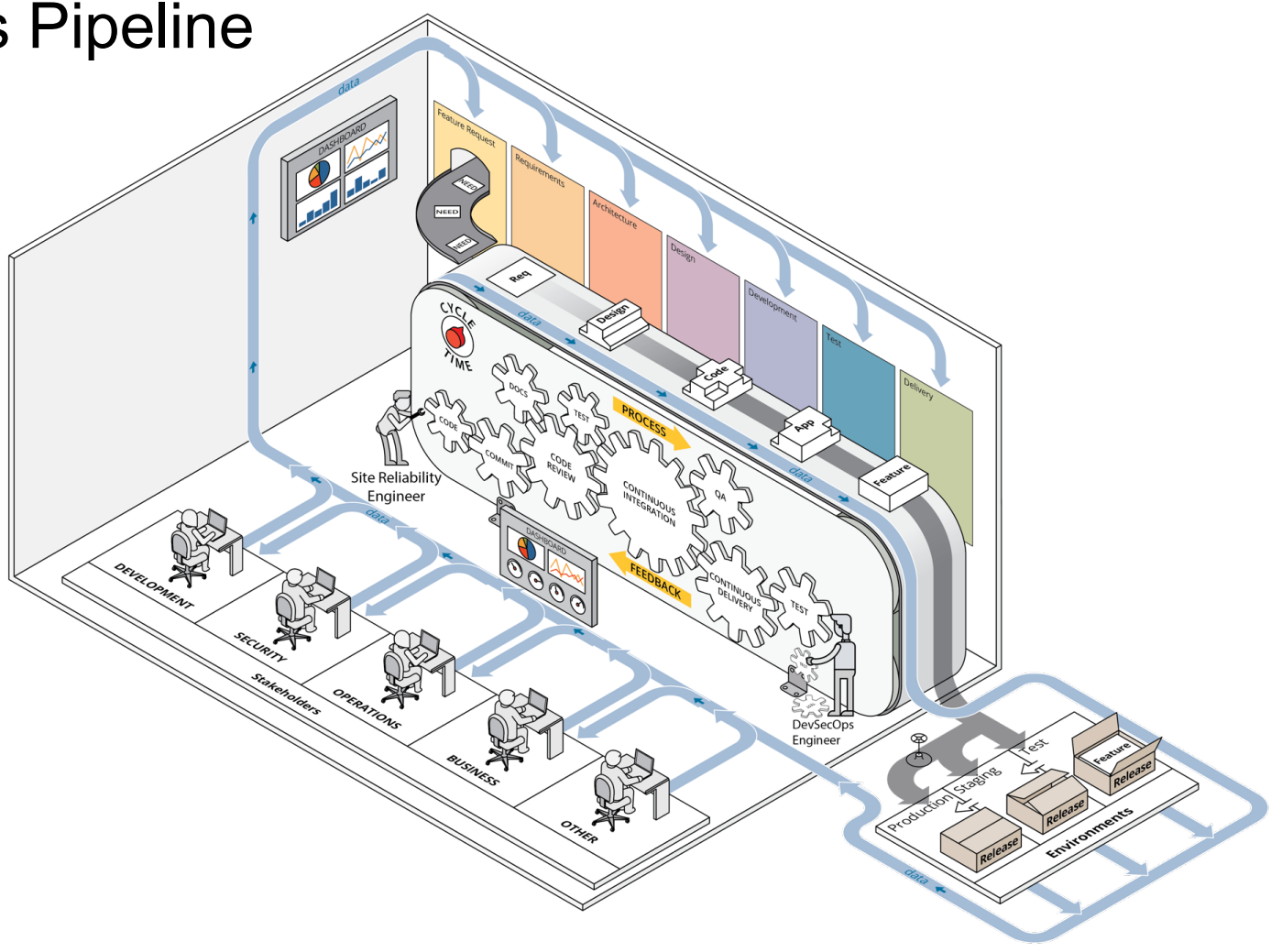
DevSecOps Infinity Diagram



© 2023 Carnegie Mellon University

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

DevSecOps Pipeline



© 2023 Carnegie Mellon University

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