

# How Many Pillars?

National CSIRT 2023

**JUNE 3, 2023**

Laurie Tyzenhaus  
CERT Coordination Center



Copyright 2023 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Homeland Security 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 sponsored by the United States Department of Defense.

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

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

DM23-0527

# Agenda

- Strategic Goals
- Operational Options
- Tactical Options
- Future Considerations

Presentation Name

# Strategic Goals

Long term planning to obtain a desired goal.

# Strategic Goals – CSIRTs, Companies, Vendors/suppliers

1. You believe cybersecurity is a serious problem and we must act.
2. You wish to avoid cyber attacks.
3. You are willing to fund and otherwise support cybersecurity measures.

Presentation Name

# Operational Plans

Creating operational or action plans to provide the structure to obtain the strategic goals.

# Operational Plans - Company

1. Supply the purchasing department with guidelines/requirements that align with the strategic goals.
2. Do your suppliers have these capabilities?
  - CVD - Coordinated Vulnerability Disclosure
  - Secure Updates – How does the vendor provide updates?
  - SBoM – Software Bill of Materials
  - End of Life/Security Support – How long will the vendor support your key devices or software?

# Operational Plans - CSIRTs

1. List the vendors or suppliers that have implemented a security portal for the customers to determine if these services are available prior to product purchasing:
  - CVD - Coordinated Vulnerability Disclosure
  - Secure Updates – How does the vendor provide updates?
  - SBoM – Software Bill of Materials
  - End of Life/Security Support – How long will the vendor support your key devices or software?



# Operational Plans – Vendor/Supplier

Supply the purchasing department with requirements that align with the Strategic goals:

- CVD - Coordinated Vulnerability Disclosure
- Secure Updates – How does the vendor provide updates?
- SBoM – Software Bill of Materials
- End of Life/Security Support – How long will the vendor support your key devices or software?

Provide the documentation which demonstrates your company's support of cybersecurity. Develop a web portal which supports the:

- Intake of vulnerability reports;
- lists updates and upgrades (\$\$) and how to obtain the software;
- provides a location to retrieve the SBoM; and
- notifies the customer in advance of end of support.

Presentation Name

# Tactical Implementation

Utilizing the operational plan to structure the implementation to support the strategic goals.

# Tactical Implementation - CSIRT

# Tactile Implementation – Vendor/Supplier

Supply the designers and developers with requirements that align with the Strategic goals:

- CVD - Coordinated Vulnerability Disclosure

- Secure Updates – How does the vendor provide updates?

- SBoM – Software Bill of Materials

- End of Life/Security Support – How long will the vendor support your key devices or software?

Provide the documentation which demonstrates your company's support of cybersecurity.

- Publish a web portal which supports the strategic goals

- Vulnerability intake, testing, mitigating or remediating the vul

Presentation Name

# Future Considerations

# Future Considerations

- International Standards Organization (ISO) is where the Strategic and Operational guidance is developed, debated, and finalized.
- NIST should update the Cybersecurity Framework (CSF) to include vulnerability report intake capability, mitigation or remediation of the vulnerability and then alerting customers of the need to update or patch.

# Future Considerations

- Encourage transparency to allow the consumer/customer to conduct their own assessment of their CSF compliance status.
- SBoM is only a starting place! Consider how companies can develop a PBoM (Production (or product)) Bill of Materials. The PBoM could include the \_\_entire\_\_ production cycle and identify dependencies. This type of information could support the customer in determining if they're vulnerable!

# Questions?

**Laurie Tyzenhaus**

Senior Member of the Technical Staff

Email: [latyzenhaus@cert.org](mailto:latyzenhaus@cert.org)

