Supply Chain Product Assurance Playbook

Prepared for Winter 2024 SSCA Forum

EXIGER

Schneider Electric

TheChertoffGroup

Enabling A More Secure World.

SSCA Winter Forum

January 24, 2024
15:30 EST

Presentation Agenda

Introduction to Product Assurance – Michele Iversen

Developing a Path Towards Verifiable Trust– Carrie Wibben

Critical Product Illuminations: Highlighted Findings– JC Herz and Cassie Crossley

Scaling for Success – Carrie Wibben

Audience Q&A

Product Assurance Playbook

Partnering to Build Trusted, Resilient Supply Chains

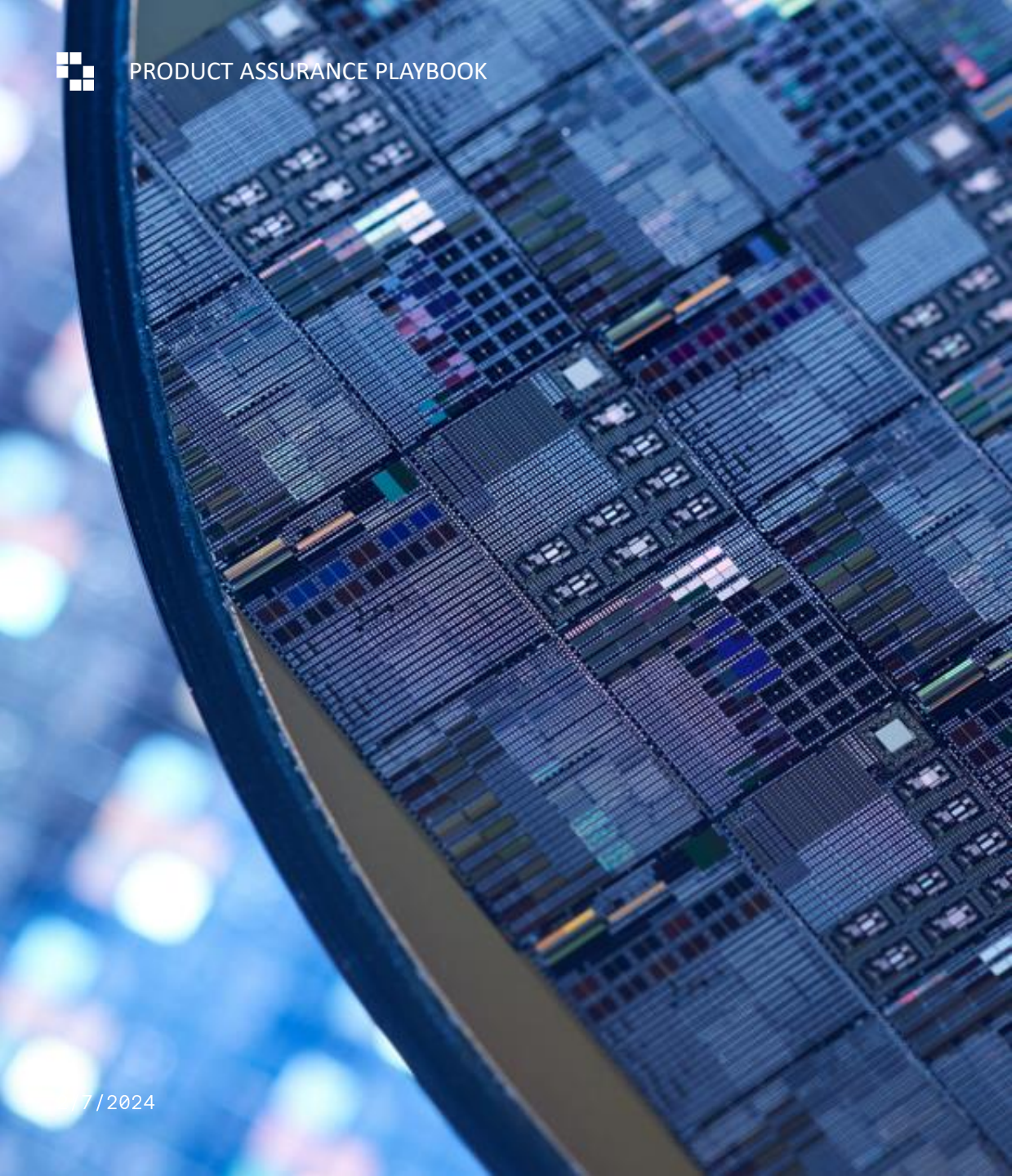
Introduction by Michele Iversen, *Director, Cybersecurity Integration, DoD CIO*

Presenting Today:

Carrie Wibben
President, Exiger Government Solutions

JC Herz
SVP, Cyber Supply Chain Exiger

Cassie Crossley
VP, Supply Chain Security Schneider Electric



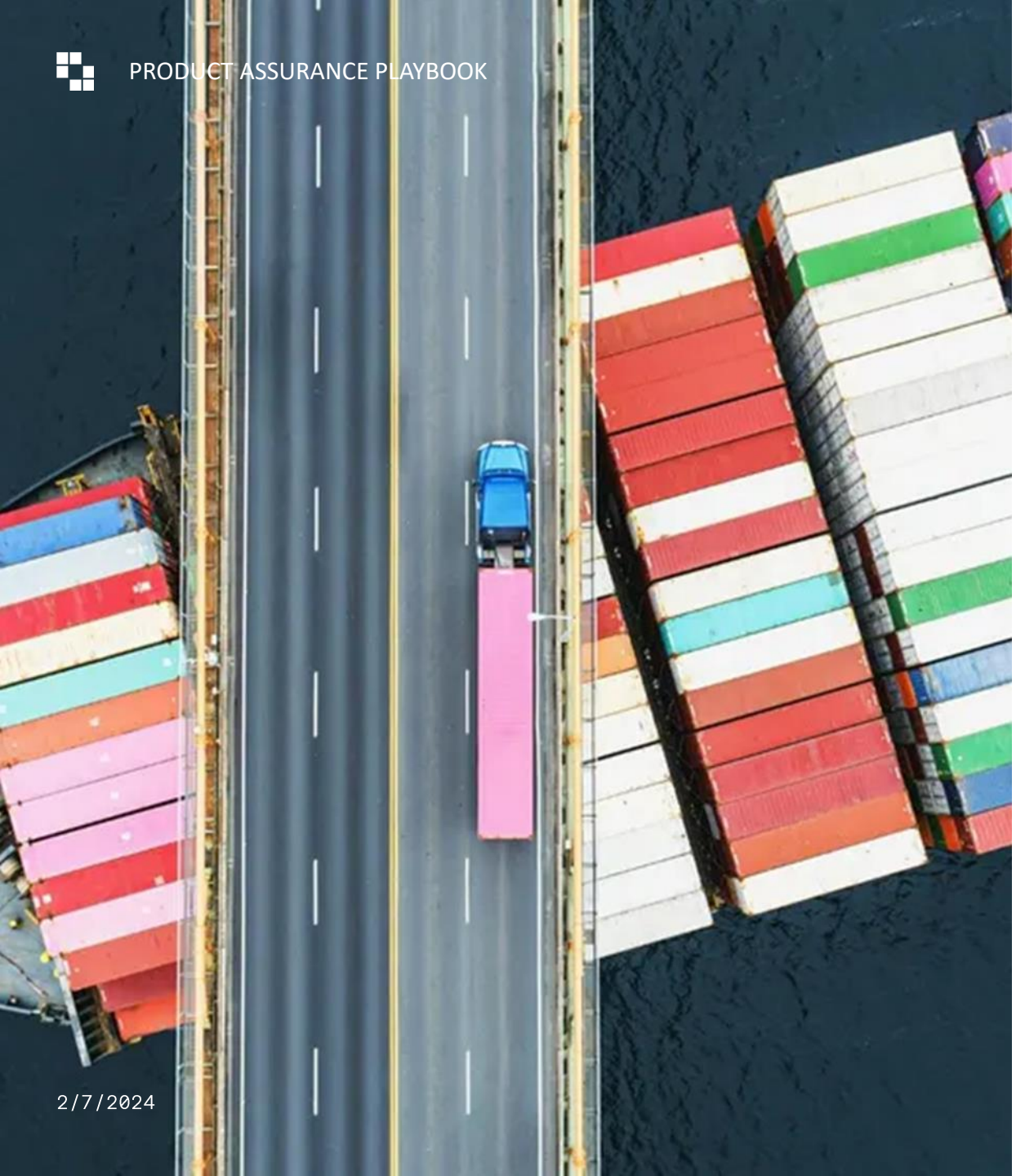
Introduction to Product Assurance

The Challenge: Validating Product Integrity

- Myriad challenges to assuring modern supply chains.
  - How to trace provenance in hardware and software supply chains.
  - Challenges in identifying, reporting, and mitigating risk, especially when the risk exists deep in the sub-tiers.
- Any successful process must be collaborative, adaptable, and relative to the criticality of the product itself and the sensitivity of the missions and functions that it supports.
  - Adopting a progressively iterative 80/20 perspective on identifying, prioritizing, and mitigating risks sufficient to be confident of mission success.
  - Establishing thresholds for acceptable levels of risk that adjust to be commensurate with the nature of the product's significance within the enterprise. For example, a product with military or national security applications would undergo greater scrutiny.

The Solution: A Comprehensive Supply Chain Product Assurance Playbook

- The **Product Assurance Playbook** is rooted in the directives and implementation of **E.O. 14028 on Improving the Nation's Cybersecurity** to enhance the Federal Government's visibility into and detection of cybersecurity vulnerabilities and threats.
- The Federal Government, and particularly the Department of Defense (DoD), is concerned about **adversarial exploitation of mission critical products and services**, including insertion of malicious code or counterfeit components within these products.
- Mission critical products that contain software or hardware with foreign association in countries of concern pose elevated risks. In this regard, the **process must assess company-level and product-level risks** with a focus on both **cybersecurity and foreign ownership, control or influence (FOCI) risks** within a vendor's organization and mission critical products' supply chain, including **provenance of software and hardware components** (i.e., countries of origin and foreign influence).
- Additionally, the process **facilitates information sharing on inherent risks between the DoD and vendors** that provide DoD with mission critical products or services. The information sharing is intended to provide DoD and other U.S. Government agencies with **transparency into a vendor's supply chain risk management (SCRM) processes**.



Developing a Path Towards Verifiable Trust

Origins of the Partnership

How Exiger, Schneider, and DoD CIO came together to work on a new approach to supply chain integrity and product assurance, so that Schneider could be unquestionably “fit for purpose” in mission-critical systems and applications.

2022 Q4

USG concerned about FOCI risks, identified in part by Exiger, within the Schneider corporate structure and supply chain.

2023 Q1

Schneider proactively invested in understanding USG perspective on identified risks, and shared mitigations already undertaken.

2023 Q2

Open dialogue initiated with DoD CIO, parallel efforts to develop remediation PLAYBOOK and illumination of critical products.

Q2–Present

Mitigations underway for completed critical product Illuminations, out-briefs of findings to DoD agencies, and multiple additional product Illuminations in progress.

Playbook Pillars

- Commit to Transparency and Trusted Partnerships
- Prioritize Critical Products
- Illuminate and Assess Risk
- Identify and Implement Mitigations to Remediate Risk
- Continuously Monitor Product for Risk Indicators

Scaling for Success

Implementing the Playbook

- Engage with suppliers in the defense, national security, and critical infrastructure industrial bases to identify additional partners and products for inclusion in the Product Assurance Playbook initiative.
- Ongoing dialogue between industry and government stakeholders on industry best practices and lessons learned as initiative is scaled.
- Expanded industry and government evolution of the process, and eventual formalization of the Product Assurance Playbook as the preferred industry standard.

For additional information, please reach out to Exiger Government Solutions

contact@exiger.com
1676 International Drive, Suite 630
McLean, VA 22102