IOT/OT STANDARDS & REGULATIONS

DESIGN. BUILD. SECURE

ELECTRO FEDERATION CANADA EFC

AGENDA

- Standards and Regulations {Singapore, EU, US, and Canada}
- Bill C-26
- Planning for this Future
- Questions

ABOUT TWELVEDOT

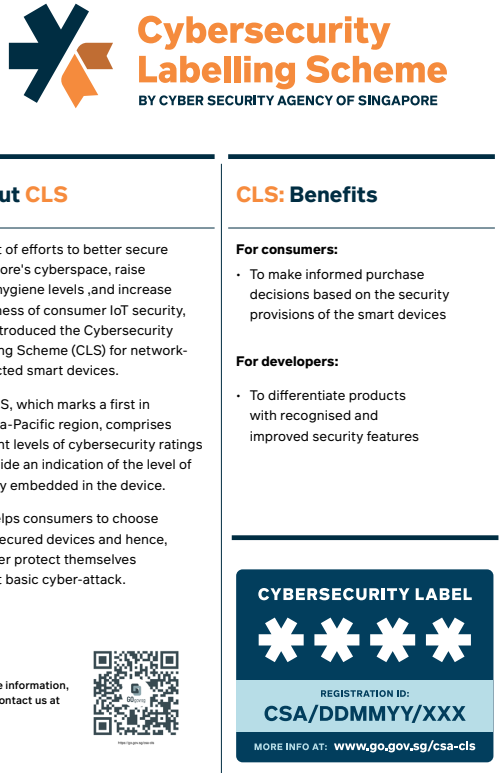
- We are an Ottawa based cyber consultancy specializing in HW and SW development and governance
  - We work with companies to improve both products and organizations
- We work with the CSA Group for testing, assessment and standards development
- Editor for ISO 27400 IoT Security and Privacy
- Co-Editor for ISO 27404 IoT Security Baseline
- Editor of IEC 30149 IoT Trustworthiness
- We have pen tested and evaluated well over 700 IoT products to date

SETTING THE STAGE

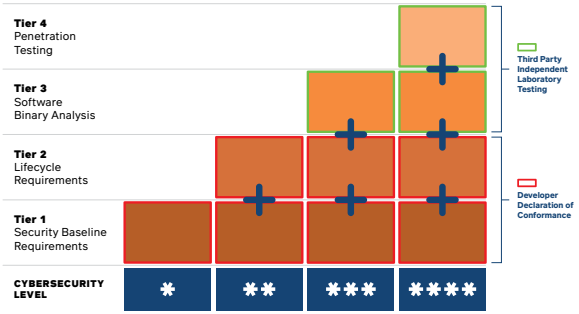
NEW EXPECTATIONS

- Many nations are developing or have implemented regulatory and certification requirements
  - Singapore, Japan, United Kingdom, EU, and Australia
  - Many regulations for x-border sectors i.e. energy (NERC & FERC)
  - Canada will not develop one but probably adopt another nations framework (C-26)
- NIST and ISO working on Baseline standards to support SMB vendors

SINGAPORE - LABELING



- Regulation launched last year
- Mandatory for some sectors
- Being pushed by UK**
- Working towards making this an ISO standard



Cybersecurity Levels

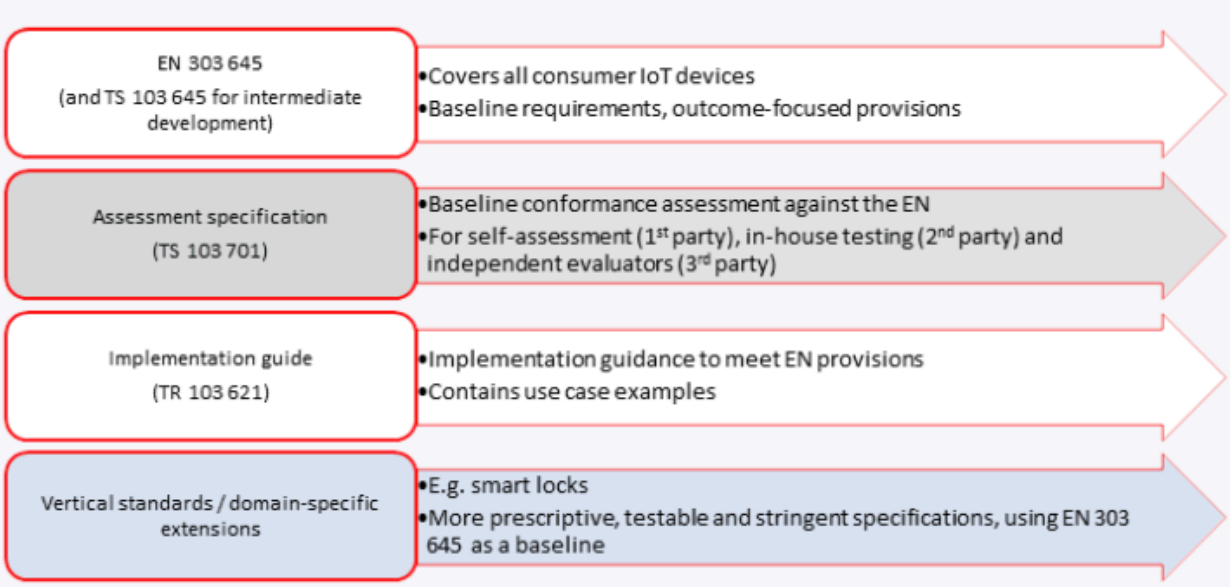
The CLS comprises of four (4) cybersecurity levels, corresponding to the number of asterisks on the label, as well as the highest assessment tier that the product has successfully completed.

There are 4 different tiers of assessment. Each assessment tier, to be completed in sequence, reflects the increasing resistance the product has to basic attacks that they may be commonly subjected to.

For example, a developer may choose to have the product rated at CLS Level 3, and hence have the product undergo assessments at Tiers 1, 2, and 3.

source: Cybersecurity_Certification_Guide_V2.pdf

EU



- Targeting consumer grade products
- Working towards a full certification scheme on this
- Evaluating some target sectors for mandatory requirements

UNITED STATES

Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order

Overview | Completed Assignments | Latest Updates

OVERVIEW

The President's Executive Order (EO) 14028 on Improving the Nation's Cybersecurity issued on May 12, 2021, charges multiple agencies – including NIST – with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain.

Section 4 directs NIST to solicit input from the private sector, academia, government agencies, and others and to identify existing or develop new standards, tools, best practices, and other guidelines to enhance software supply chain security. Those guidelines, **which are ultimately aimed at federal agencies but which also are available for industry and others to use**, include:

- criteria to evaluate software security,
- criteria to evaluate the security practices of the developers and suppliers, and
- innovative tools or methods to demonstrate conformance with secure practices.

NIST is to consult with other agencies in producing some of its guidance; in turn, several of those agencies are directed to take steps to ensure that federal procurement of software follows that guidance.

The EO also assigns NIST to work on two labeling efforts related to consumer Internet of Things (IoT) devices and consumer software with the goal of **encouraging manufacturers to produce – and purchasers to be informed about**– products created with greater consideration of cybersecurity risks and capabilities.

COMPLETED

NIST solicited input from the private sector, academia, government agencies, and others through multiple requests for position papers, comments on drafts, presentations, and discussions at heavily attended virtual workshops, briefings and listening sessions. These engagements informed all of NIST's actions under Section 4.

NIST consulted with the National Security Agency (NSA), Office of Management and Budget (OMB), Cybersecurity & Infrastructure Security Agency (CISA), and the Director of National Intelligence (DNI) and then defined "critical software" by June 26, 2021.

- Consumer labeling program
- SDLC for labeling program
- Evaluating some target sectors for mandatory requirements
- Supply chain risk mgmt

https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

https://www.nist.gov/system/files/documents/2022/07/11/Report to President - Improving the Nations Cybersecurity.pdf

Standards and Regulations

A NATIONAL SECURITY PERSPECTIVE

Communications Security Establishment (CSE) and international partners publish joint guide on secure-by-design and -default principles

From: Canadian Centre for Cyber Security

April 13, 2023

CSE's Canadian Centre for Cyber Security (Cyber Centre) joined the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the following international partners to provide recommendations for Information Technology (IT) manufacturers to use secure by design and secure by default principles in the development of their products:

- Australian Cyber Security Centre (ACSC)
- New Zealand: Computer Emergency Response Team New Zealand (CERT NZ)
- New Zealand National Cyber Security Centre (NZ NCSC)
- United Kingdom's National Cyber Security Centre (NCSC-UK)
- Germany's Federal Office for Information Security (BSI)
- Netherlands National Cyber

The new guide emphasizes the need to shift the burden of cyber security risk away from the customer and instead encourage technology manufacturers to design safe products that are secure by design and by default.

PRESS RELEASE

U.S. and International Partners Publish Secure-by-Design and -Default Principles and Approaches

Released: April 13, 2023

Joint product outlines clear steps that technology providers can take to increase the safety of products used around the world

WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the cybersecurity authorities of Australia , Canada , United Kingdom , Germany , Netherlands , and New Zealand (CERT NZ , NCSC-NZ) published today "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default." This joint guidance urges software manufacturers to take urgent steps necessary to ship products that are secure-by-design and -default. To create a future where technology and associated products are safe for customers, the authoring agencies urge manufacturers to revamp their design and development programs to permit only secure-by-design and -default products to be shipped to customers.

https://www.cisa.gov/news-events/news/us-and-international-partners-publish-secure-design-and-default-principles-and-approaches

Standards and Regulations

BILL C-26

UNDERSTANDING THE BASICS

- Current edits {subject to debate in HoC}
- Targeted sectors: {energy, telecom, nuclear, transport, banking, }
- Mandatory:
  - Establish a cyber security program
  - Immediately reporting compromises
  - Mitigate supply-chain and 3rd party risks
  - Maintaining compliance records

UNDERSTANDING THE BASICS - C-26

- Concepts
  - Cyber Center will provide vendors/providers support
  - Will be implemented via ISED
  - Enforcement aspects still being defined
  - Readiness assessment
  - Cyber baselines for operations, products, services including supply chain
  - Security by design approach

https://www.parl.ca/legisinfo/en/bill/44-1/c-26

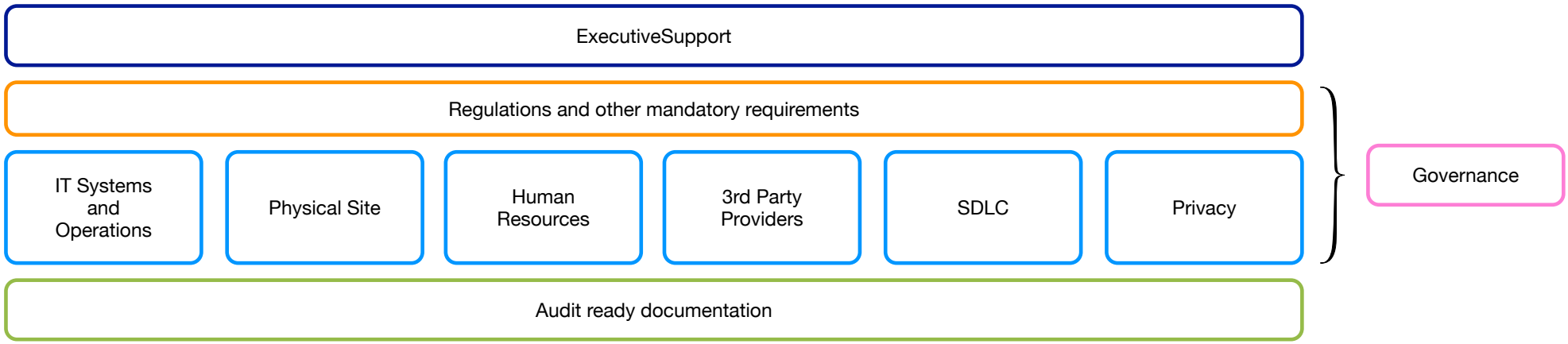
CREATING YOUR PLAN

START SMALL AND GROW THE PRACTICE

- Get to know how these regulations will impact your specific business
- Start small:
  - *Assess your current risk posture for the business and products being developed*
  - *Create a draft strategy/plan to get the necessary improvements*
  - *Ensure you document any/all regulations that will impact your business*
- Security test and evaluate your product to understand what a “hacker” sees
- Provide your staff training on the identified risks and how to prevent and report

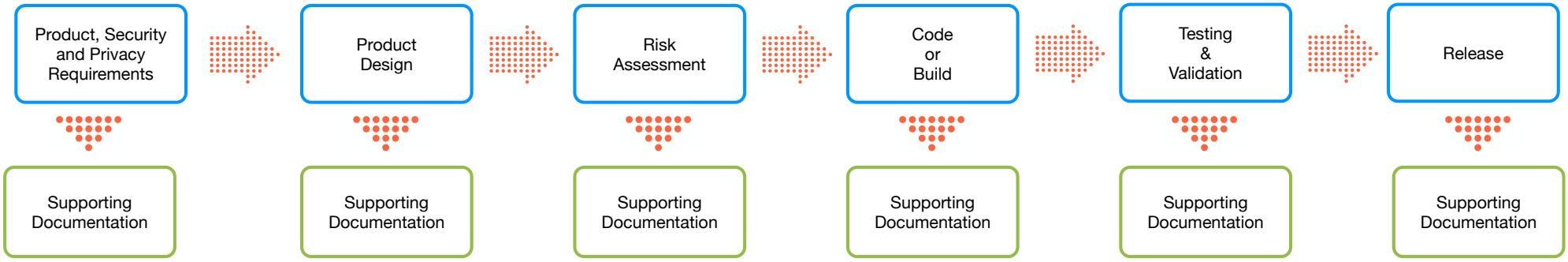
Goal: Get ahead of the curve to limit business impacts

STARTING MODEL



Standards and Regulations

SECURE APPROACH TO DEVELOPMENT



Standards and Regulations

OPEN DISCUSSION

Questions

or

Comments

Contact: security@twelvedot.com

DESIGN. BUILD. SECURE

security@twelvedot.com
@encrypto99
www.twelvedot.com