ORY / summit-22

Harri Hursti

Head of Security

✉ harri@ory.sh

@ScoF

# Governments are now mandating Zero Trust and Software Supply Chain Security. What to they want?

## Executive Order 14028

October 20th 2022

# What kickstarted Zero Trust?

Intelligence …

- While Snowden affair was not a starting point, it was a contributor and an accelerator
- ZT is now pushed by National Security interests of many nations

# Mega-trends of war and crime accelerating in 2022

## Open Source Intelligence used as targeting and recon tools

- The Castle-and-Moat is meaningless if the attacker is ignoring the Moat.
- Open Source Intelligence recon is changed the playfield

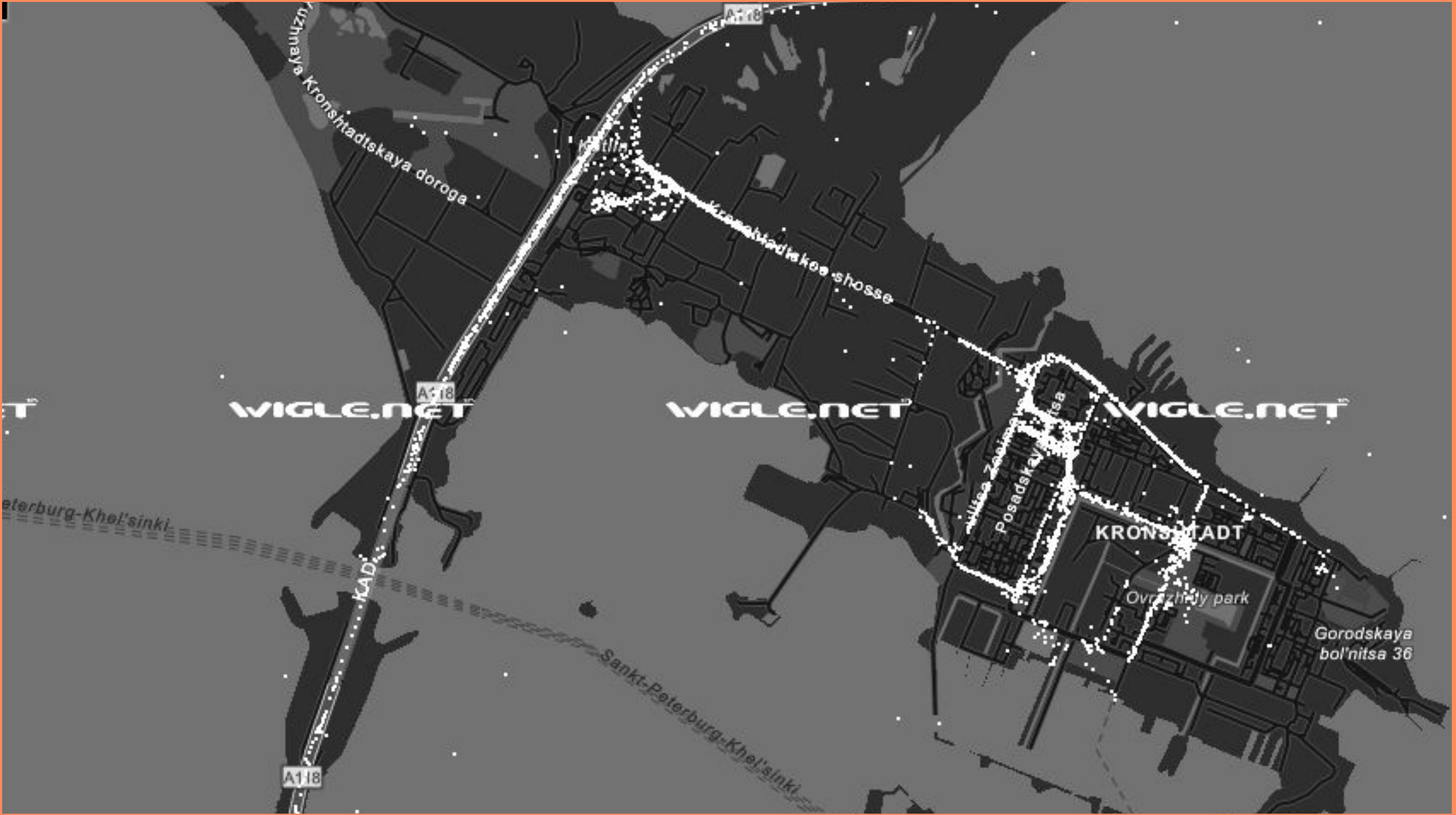
# Mega-trends of war and crime accelerating in 2022

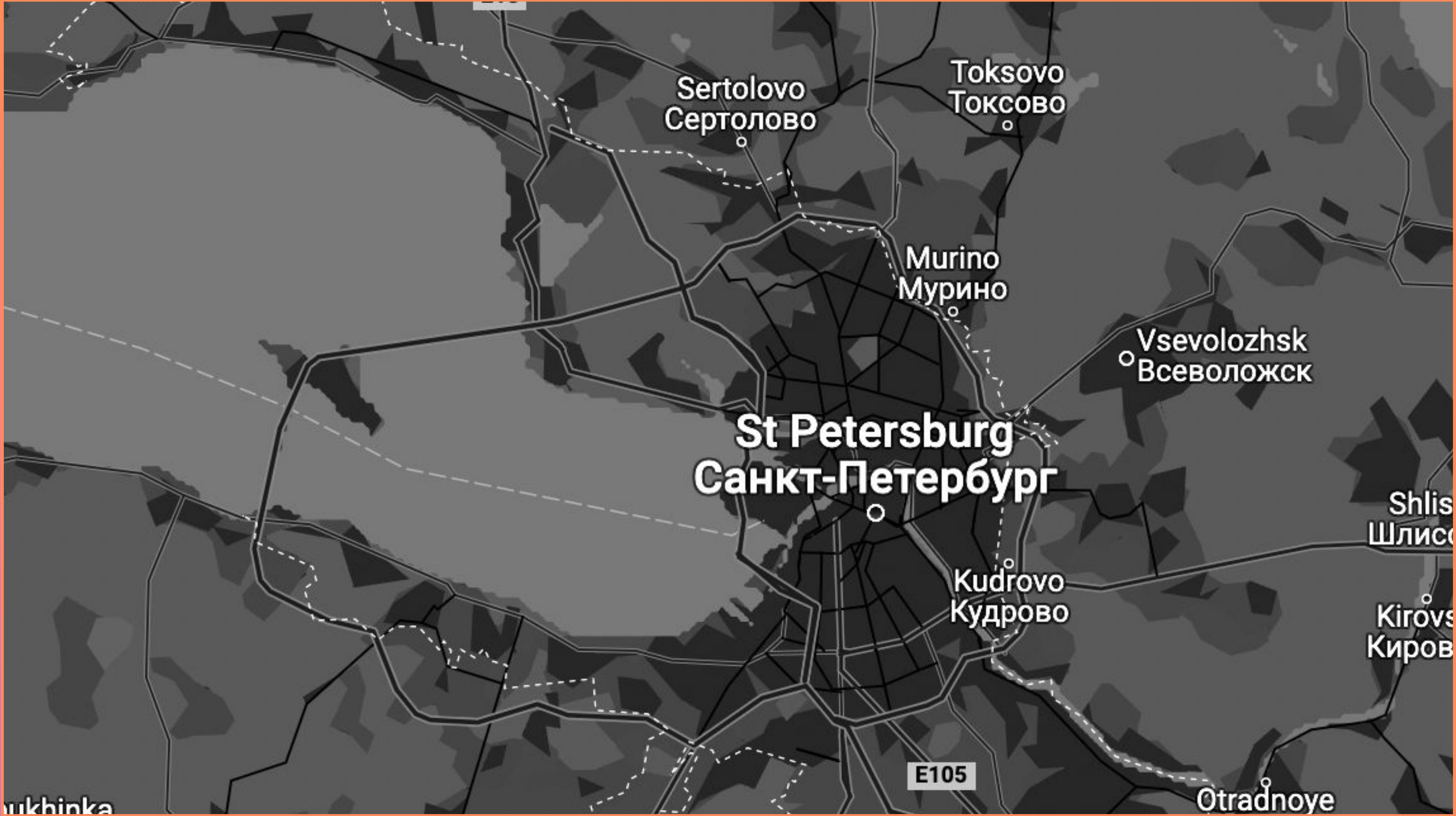
- McKinsey, 4 megatrends
  - ZTA
  - Digital Identity
  - Privacy Engineering
  - Explainable AI (XAI)

- … see who is missing…

# Mega-trends of war and crime accelerating in 2022

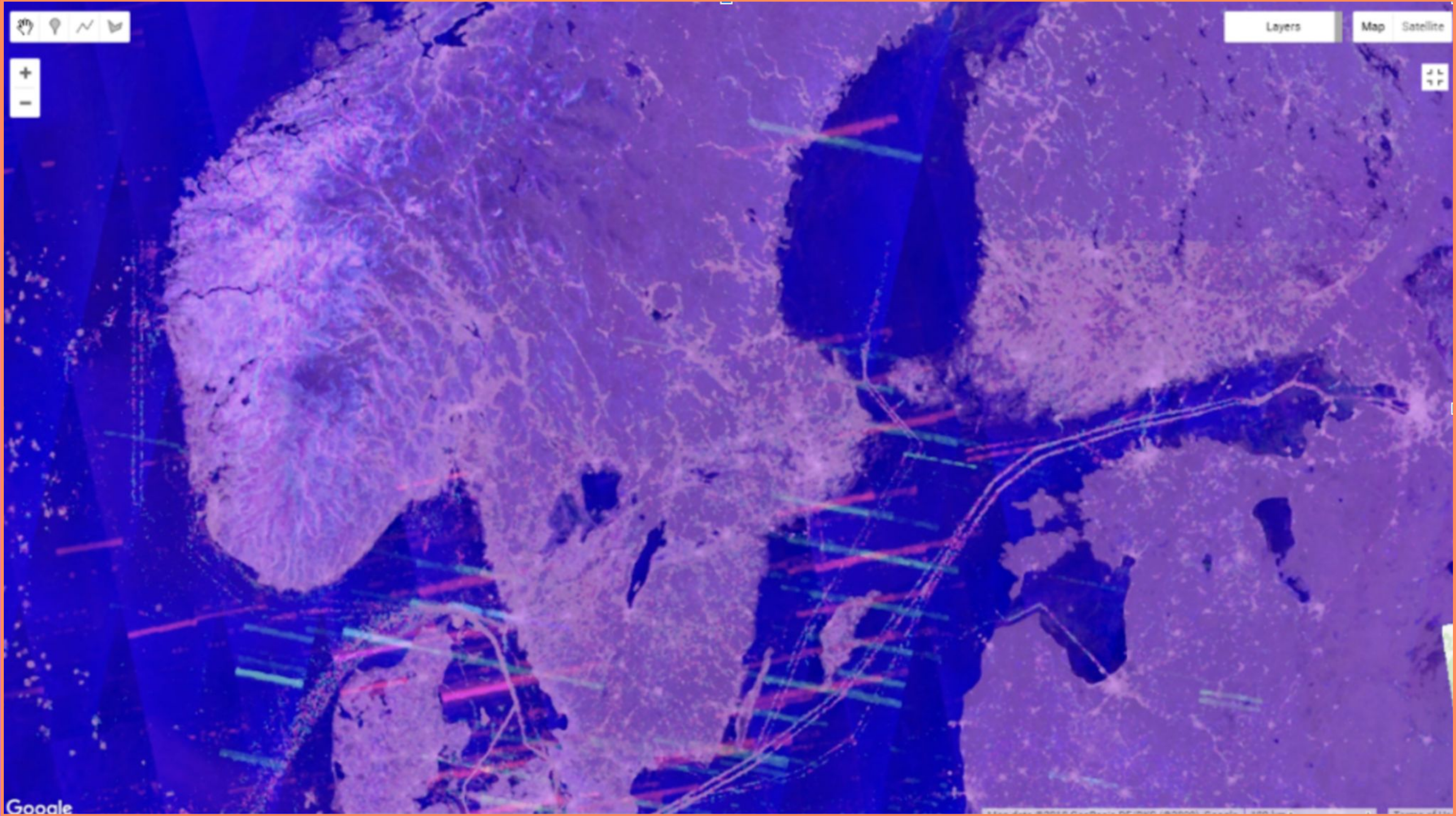
- Examples
  - Shodan
  - Censys
  - GreyNoise
  - robtex
  - WiGLE
  - RadioCells
  - Spiderfoot


A118
Yuzhnaya Kronshtadtskaya doroga
Kotlin
Kronshtadtskoe shosse
A118
WIGLE.NET
WIGLE.NET
WIGLE.NET
ulitsa Zosimova
Posadskaya ulitsa
KRONSHTADT
Ovrazhniy park
Gorodskaya bol'nitsa 36
eterburg-Khel'sinki
KAD
Sankt-Peterburg-Khel'sinki
A118


Sertolovo
Сертолово
Toksovo
Токсово
Murino
Мурино
Vsevolozhsk
Всеволожск
St Petersburg
Санкт-Петербург
Shlis
Шлисс
Kudrovo
Кудрово
Kirovs
Киров
E105
Otradnoye
ukhinka

# Mega-trends of war and crime accelerating in 2022

- Similar sets of information sources are available for about all imaginable areas of interest
- Ukraine War boosted OSINT value
- Innovative new uses
    - Using commercial SAR images to find radars with RIT Open Source SW


Layers
Map
Satellite
+
−
Google

# Cyberwar and IOps- 5th and 6th domains of the war

Cyber and Information spaces are different

- ➡ All other domains we fight wars:
  - Air
  - Land
  - Sea (and underwater)
  - Space
  - are natural domains with the laws of physics and nature

# Cyberwar and IOps- 5th and 6th domains of the war

➡ Cyberspace and Information space are the only man-made war theatres

- No distance
- No universal clock
- IS is living in our minds rent-free
- Attribution is usually extremely difficult

and we have not agreed on laws or rules of engagement

# Cyberwar and IOps- 5th and 6th domains of the war

- Zero Trust harmonizes the defenses between Cyberspace and Information space
  - Traditional Cybersecurity measures are not effective defenses against Information space operations

# Mega-trends of war and crime accelerating in 2022

One of the most consequential years

- USB - WiFi - other connectivity
- Barcodes
- SDR (and other TTPs accelerating side channel attacks)
- Social Engineering in industrial scale
- Crime-as-a-Service, especially Ransomware-as-a-Service
- Further Weaponization of Social Media
    - War by Other Means: Influence Warfare Subverts Democracy
- Firmware attacks
- Hardware attacks
    - Supply chain attacks are getting harder to detect
    - Foundries are getting compromised

# Why are we talking about this today?

This is nothing new?

- What are the roots of Zero Trust, the industry edition?
  - 1994 - The term "zero trust" was coined by Stephen Paul Marsh in his doctoral thesis on computer security at the University of Stirling.
  - 2004 - Jericho Forum, discussing the trend of what was then coined "de-perimeterization"
  - 2009 - Google starts implementing BeyondCorp
  - 2010 - John Kindervag, father of Zero Trust, coining the term into the broader knowledge

  **Snowden affair started 2013**

  - 2014 - Google BeyondCorp Paper
  - 2017 - O'Reilly Zero Trust Networks
  - 2018 - NIST and NCCoE led to the publication of SP 800-207, Zero Trust Architecture
  - 2019 - Google Zanzibar research paper
- In the context of security, this term is ancient. It must be well understood then?

# Why are we talking about this today?

Milestones of the term

In 2010, John Kindervag, an analyst at Forrester Research, coined the term "zero trust", which centered around the idea that an organization shouldn't trust anything inside or outside its perimeters. In the zero trust model, all network traffic is untrusted no matter its origin.

In 2014, Google rolled out BeyondCorp, the search giant's implementation of the zero trust security model that shifted access controls from the network perimeter to individual users and devices.

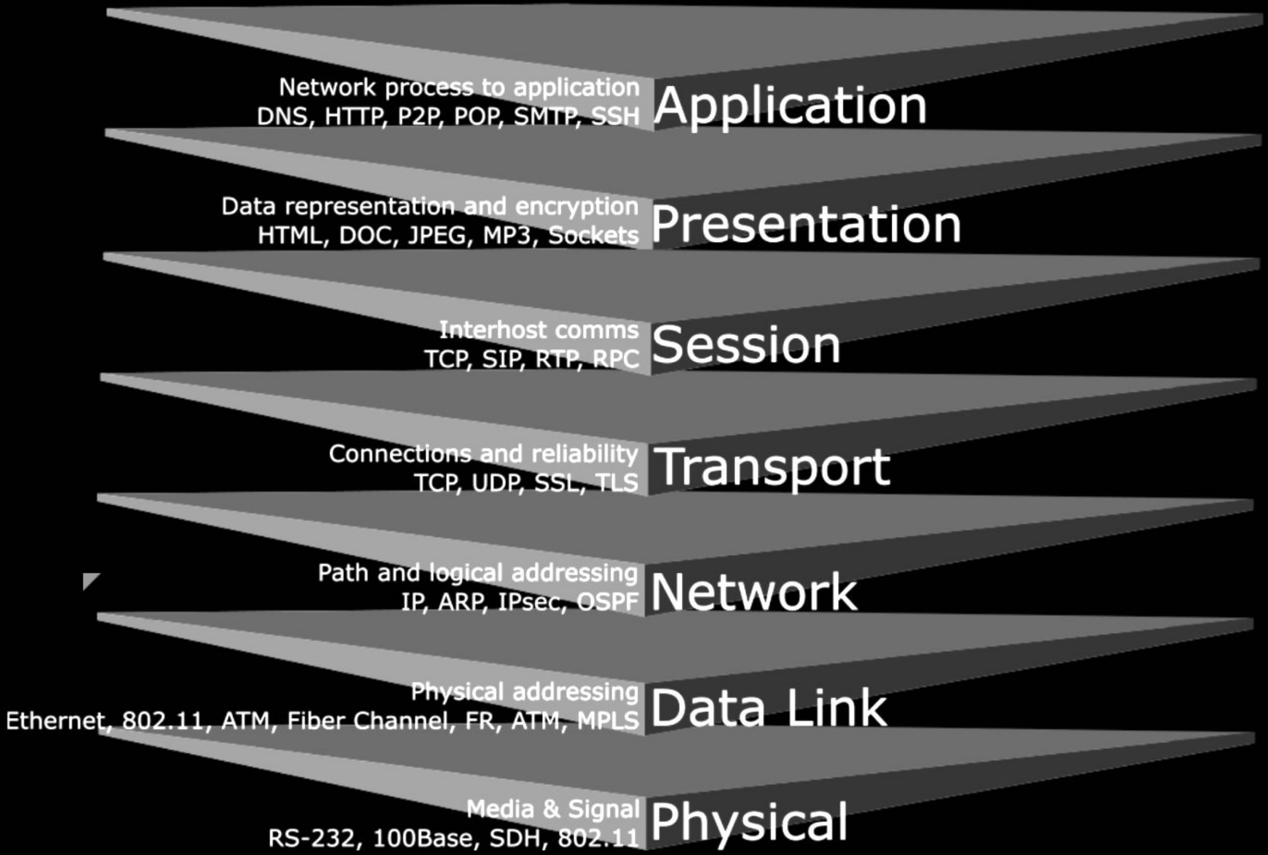
A 2019 Google blog lists the three main principles of BeyondCorp as:

1. Connecting from a particular network does not determine which service you can access.
2. Access to services is granted based on what the infrastructure knows about you and your device.
3. All access to services must be authenticated, authorized and encrypted for every request.
    - The initial access validation revalidated for each request

# Why are we talking about this today?

What is the urgency?

- Zero Trust (ZT) is never about fixing one layer and trusting the others
    - Zero Trust must assume that all layers are compromised
        - Adding words “Zero Trust” does not make your favorite layer more secure
        - Many things ZT seems today to be just marketing
        - Definition of “layer” has become more complex
        - Enterprises have sensitive assets distributed across different environments in their network, including critical applications running on bare-metal, traditional servers, cloud-hosted virtual machines, containerized workloads, and other host systems. Organizations lack visibility into what assets are in their network, where data exists in their distributed environment, who has access to data, and how the data is secured from malicious or unauthorized access



Network process to application
DNS, HTTP, P2P, POP, SMTP, SSH
Application

Data representation and encryption
HTML, DOC, JPEG, MP3, Sockets
Presentation

Interhost comms
TCP, SIP, RTP, RPC
Session

Connections and reliability
TCP, UDP, SSL, TLS
Transport

Path and logical addressing
IP, ARP, IPsec, OSPF
Network

Physical addressing
Ethernet, 802.11, ATM, Fiber Channel, FR, ATM, MPLS
Data Link

Media & Signal
RS-232, 100Base, SDH, 802.11
Physical

Exploit

Phishing

Hijacking

Reconnaissance / DOS

MITM

Spoofing

Sniffing

# Why are we talking about this today?

What is the urgency?

- RSA conference in June 2022
  - About ⅓ of companies on the show floor advertised to sell something “Zero Trust”
  - Interviewing them randomly, all top 5 offerings had nothing to do with Zero Trust
  - Most common wrong and/or missing the big picture answers were:
    - Passwordless, Zero Trust means that users log in using certificates instead of passwords
    - Multi-factor authentication, Zero Trust means that app or physical dongle is used
    - Certificate management, they track all certificates and their uses and expiration dates and make sure that certificates are renewed in time
    - Cloud management, they manage user credential for hybrid cloud deployments
    - Kubernetes management, they make dynamic clusters trustworthy
  - I assumed that different add-on overlay network storied would be prominent, but no more…
    - None of the top 5 explanations included anything about edgeless network, tokens, or continuous validation.

# Why are we talking about this today?

What is the urgency?

- New definitions of Zero Trust expand to address concerns in Software Supply Chain
  - Open Source has become a key answer to provide transparency required
    - Open Sourcing SDK has become the marketing snake oil to blur it
  - Recognizing the value of Open Standards and Protocols is increasing

Zero Trust is still commonly misunderstood as software centric model due to lack of understanding the relationship between hardware and software today (hardware is the new software)

# From Zero Knowledge Proofs to Zero Trust Architecture

What are we talking about?

- Innovation in security philosophy has been very limited. Buzzwords came and went, but this time we are changing the fundamentals
    - Today we are between “Sign-In And Then Ignore” and “Trust, But Verify”
    - Zero Trust is “Never Trust Always Verify”
    - User, subjects, everyone is always assumed to be hostile
    - Edgeless network
    - Continuous verification
        - Tokenization of security
    - Contextualization of all request
        - Least permissions principle
- Until now, we have been <u>IGNORING</u> the usability aspect of the security
    - Convenience always wins over security
    - More studies about usability of security are needed

# From Zero Knowledge Proofs to Zero Trust Architecture

What we are talking about?

- Most important is the change in philosophy:
    - Protection of Crown Jewels
        - Digital assets (files, data, etc)
        - Workflows (workloads, APIs, processes, etc)
    - No longer protection or implied trust
        - Based on logical location (server, network, etc)
        - No assumption of perimeter defences (network, credentials, etc)
- Identity is the cornerstone
    - Everything needs to have one
- Open Source
- Open Standards
- Interoperability
- Privacy and anonymity preserving Strong ID

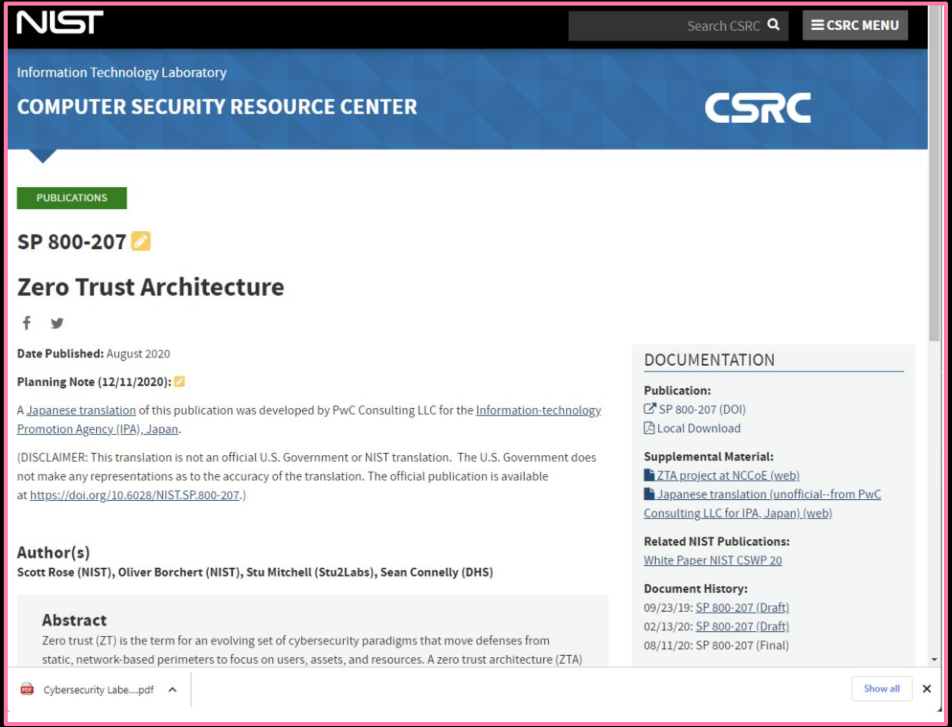
# Why we talking about this today?

What is the urgency?

- When, other than the Great Gold Rush, has there been so much confusion?
    - Zero Trust is an ever evolving term to cover set of massive paradigm changes in Cyber Security
        - It was originally conceived as response to Enterprise Security model changes
            - Cloud
            - BYOD
            - Covid
            - Ukraine war
    - Zero Trust is not a product, it is a journey
        - Current cornerstone definition document was drafted before COVID
        - We will continue to redefine what the term means as new threats emerge
    - Zero Trust starts from rethinking security model as a whole
        - Implementation of Zero Trust tools without changing the mental model is likely to weaken the security posture
        - It is common to keep on operating with “LDAP model” while transitioning to tokens

# Why are we talking about this today?

- Standard



Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

SP 800-207

Zero Trust Architecture

**Date Published:** August 2020

**Planning Note (12/11/2020):**

A Japanese translation of this publication was developed by PwC Consulting LLC for the Information-technology Promotion Agency (IPA), Japan.

(DISCLAIMER: This translation is not an official U.S. Government or NIST translation. The U.S. Government does not make any representations as to the accuracy of the translation. The official publication is available at https://doi.org/10.6028/NIST.SP.800-207.)

Author(s)

**Scott Rose (NIST), Oliver Borchert (NIST), Stu Mitchell (Stu2Labs), Sean Connelly (DHS)**

Abstract

Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA)

DOCUMENTATION

**Publication:**
SP 800-207 (DOI)
Local Download

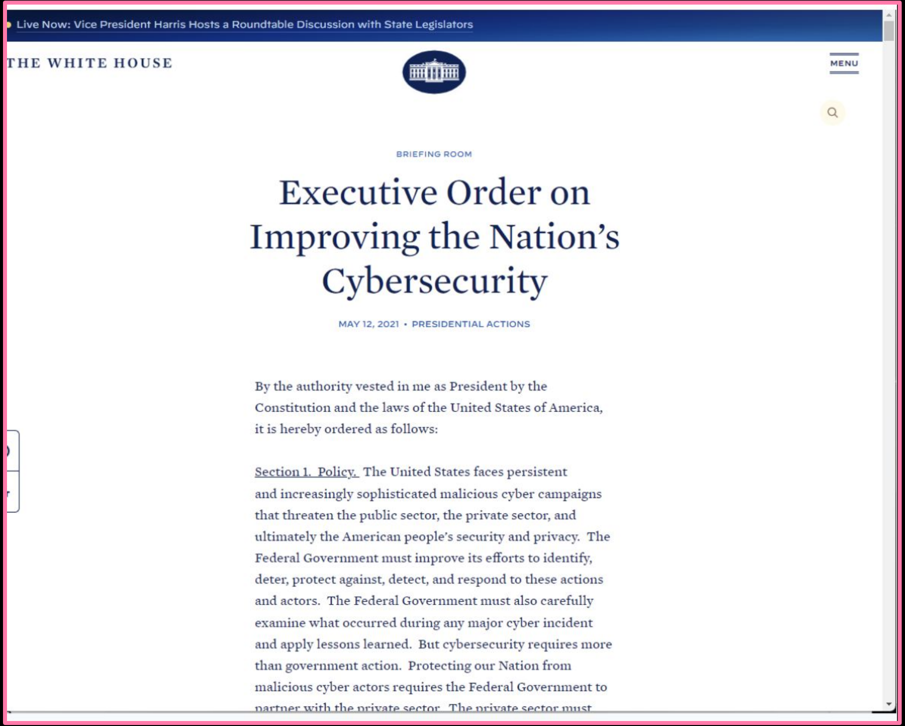
**Supplemental Material:**
ZTA project at NCCoE (web)
Japanese translation (unofficial--from PwC Consulting LLC for IPA, Japan) (web)

**Related NIST Publications:**
White Paper NIST CSWP 20

**Document History:**
09/23/19: SP 800-207 (Draft)
02/13/20: SP 800-207 (Draft)
08/11/20: SP 800-207 (Final)

# Why are we talking about this today?

- May 12, 2021
  Executive Order 14028



Live Now: Vice President Harris Hosts a Roundtable Discussion with State Legislators

THE WHITE HOUSE

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

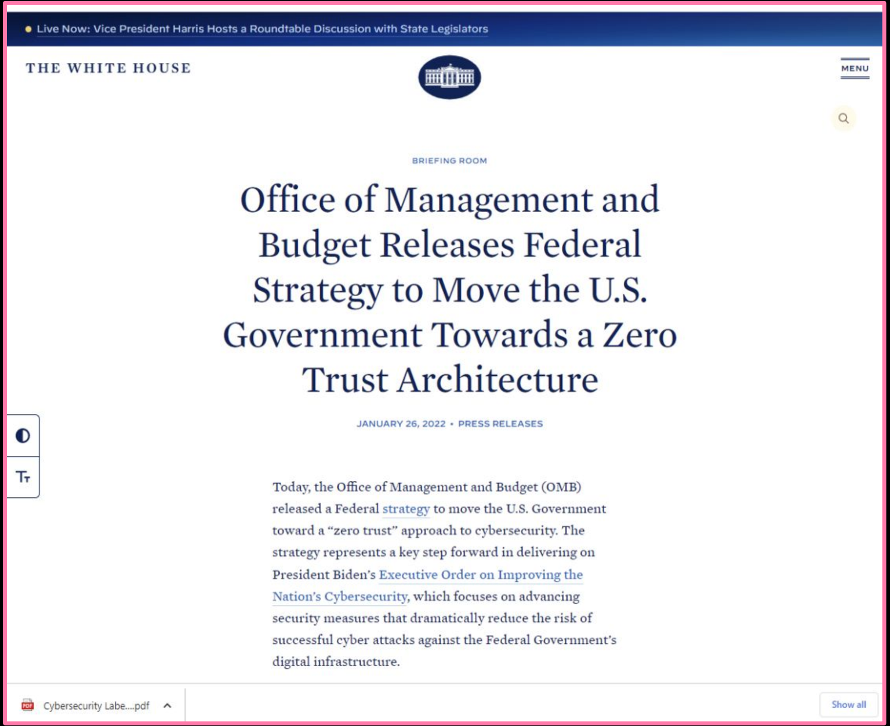
MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must

# Why are we talking about this today?

- Jan 26,2022: Strategy published
- Implementation required to be complete by End of FY24



Live Now: Vice President Harris Hosts a Roundtable Discussion with State Legislators

THE WHITE HOUSE

MENU

BRIEFING ROOM

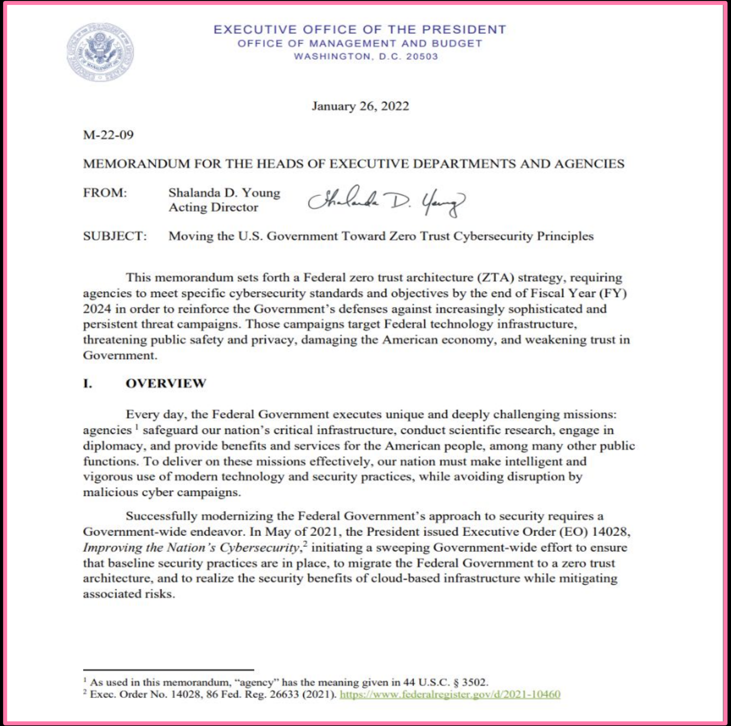
Office of Management and Budget Releases Federal Strategy to Move the U.S. Government Towards a Zero Trust Architecture

JANUARY 26, 2022 • PRESS RELEASES

Today, the Office of Management and Budget (OMB) released a Federal strategy to move the U.S. Government toward a "zero trust" approach to cybersecurity. The strategy represents a key step forward in delivering on President Biden's Executive Order on Improving the Nation's Cybersecurity, which focuses on advancing security measures that dramatically reduce the risk of successful cyber attacks against the Federal Government's digital infrastructure.

# Why are we talking about this today?

- Jan 26, 2022: Strategy published



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director
Shalanda D. Young

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

**I. OVERVIEW**

Every day, the Federal Government executes unique and deeply challenging missions: agencies [1] safeguard our nation's critical infrastructure, conduct scientific research, engage in diplomacy, and provide benefits and services for the American people, among many other public functions. To deliver on these missions effectively, our nation must make intelligent and vigorous use of modern technology and security practices, while avoiding disruption by malicious cyber campaigns.

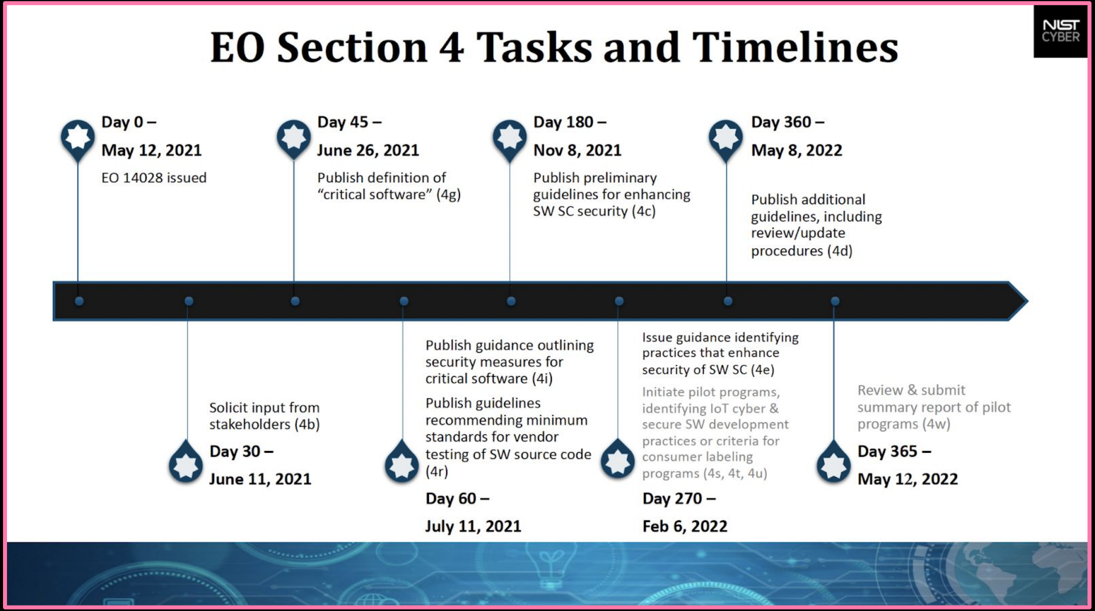
Successfully modernizing the Federal Government's approach to security requires a Government-wide endeavor. In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*,[2] initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero trust architecture, and to realize the security benefits of cloud-based infrastructure while mitigating associated risks.

[1] As used in this memorandum, "agency" has the meaning given in 44 U.S.C. § 3502.
[2] Exec. Order No. 14028, 86 Fed. Reg. 26633 (2021). https://www.federalregister.gov/d/2021-10460

# Why are we talking about this today?

What is the urgency?

- May 12, 2021: Executive Order 14028



## EO Section 4 Tasks and Timelines

NIST CYBER

**Day 0 –**
**May 12, 2021**
EO 14028 issued

**Day 30 –**
**June 11, 2021**
Solicit input from stakeholders (4b)

**Day 45 –**
**June 26, 2021**
Publish definition of "critical software" (4g)

**Day 60 –**
**July 11, 2021**
Publish guidance outlining security measures for critical software (4i)
Publish guidelines recommending minimum standards for vendor testing of SW source code (4r)

**Day 180 –**
**Nov 8, 2021**
Publish preliminary guidelines for enhancing SW SC security (4c)

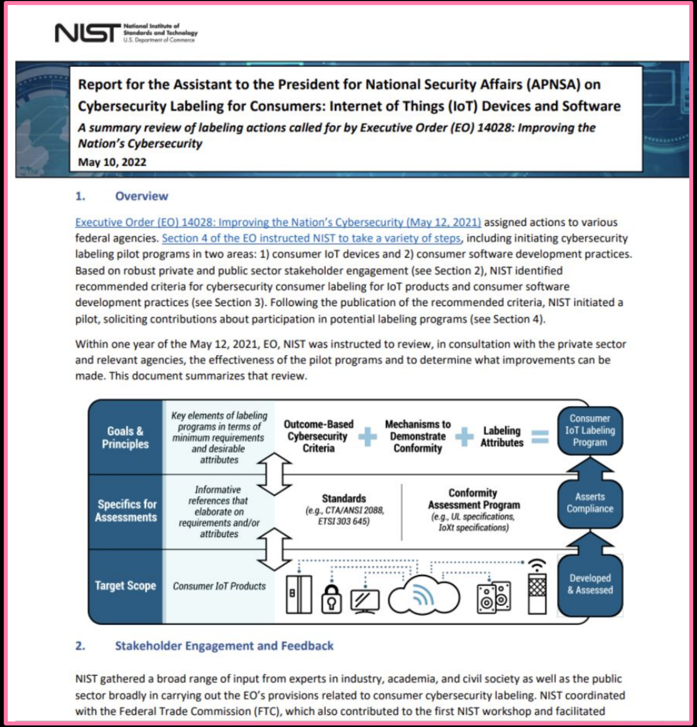
**Day 270 –**
**Feb 6, 2022**
Issue guidance identifying practices that enhance security of SW SC (4e)
Initiate pilot programs, identifying IoT cyber & secure SW development practices or criteria for consumer labeling programs (4s, 4t, 4u)

**Day 360 –**
**May 8, 2022**
Publish additional guidelines, including review/update procedures (4d)

**Day 365 –**
**May 12, 2022**
Review & submit summary report of pilot programs (4w)

# Why are we talking about this today?

- More to follow



NIST National Institute of Standards and Technology U.S. Department of Commerce

**Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software**

***A summary review of labeling actions called for by Executive Order (EO) 14028: Improving the Nation's Cybersecurity***

**May 10, 2022**

## 1. Overview

Executive Order (EO) 14028: Improving the Nation's Cybersecurity (May 12, 2021) assigned actions to various federal agencies. Section 4 of the EO instructed NIST to take a variety of steps, including initiating cybersecurity labeling pilot programs in two areas: 1) consumer IoT devices and 2) consumer software development practices. Based on robust private and public sector stakeholder engagement (see Section 2), NIST identified recommended criteria for cybersecurity consumer labeling for IoT products and consumer software development practices (see Section 3). Following the publication of the recommended criteria, NIST initiated a pilot, soliciting contributions about participation in potential labeling programs (see Section 4).

Within one year of the May 12, 2021, EO, NIST was instructed to review, in consultation with the private sector and relevant agencies, the effectiveness of the pilot programs and to determine what improvements can be made. This document summarizes that review.

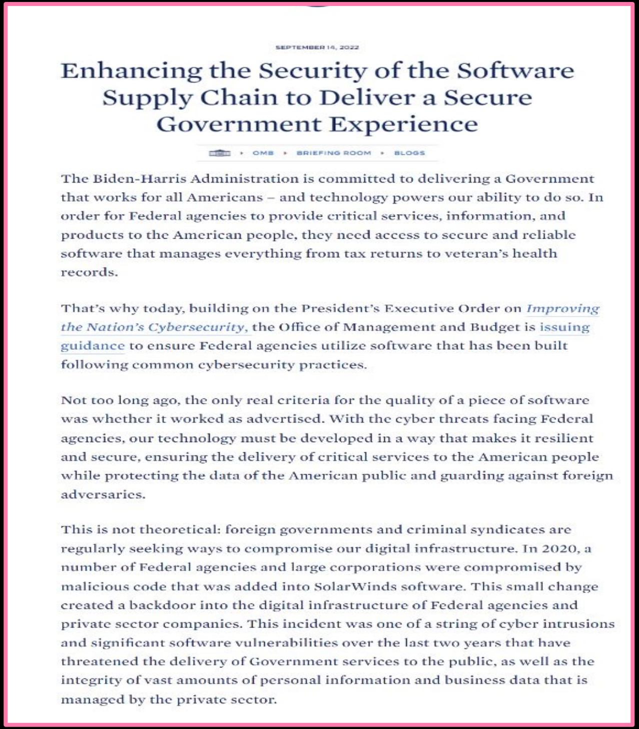
Goals & Principles
Key elements of labeling programs in terms of minimum requirements and desirable attributes
Outcome-Based Cybersecurity Criteria
+
Mechanisms to Demonstrate Conformity
+
Labeling Attributes
=
Consumer IoT Labeling Program
Specifics for Assessments
Informative references that elaborate on requirements and/or attributes
Standards (e.g., CTA/ANSI 2088, ETSI 303 645)
Conformity Assessment Program (e.g., UL specifications, IoXt specifications)
Asserts Compliance
Target Scope
Consumer IoT Products
Developed & Assessed

## 2. Stakeholder Engagement and Feedback

NIST gathered a broad range of input from experts in industry, academia, and civil society as well as the public sector broadly in carrying out the EO's provisions related to consumer cybersecurity labeling. NIST coordinated with the Federal Trade Commission (FTC), which also contributed to the first NIST workshop and facilitated

# Why are we talking about this today?

- More to follow September 14th, 2022



SEPTEMBER 14, 2022

## Enhancing the Security of the Software Supply Chain to Deliver a Secure Government Experience

The Biden-Harris Administration is committed to delivering a Government that works for all Americans – and technology powers our ability to do so. In order for Federal agencies to provide critical services, information, and products to the American people, they need access to secure and reliable software that manages everything from tax returns to veteran's health records.

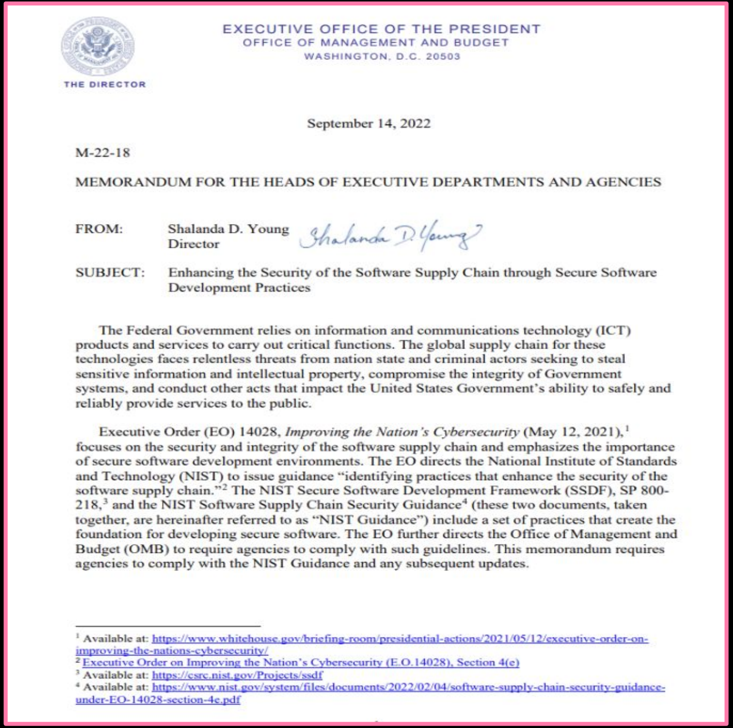
That's why today, building on the President's Executive Order on *Improving the Nation's Cybersecurity*, the Office of Management and Budget is issuing guidance to ensure Federal agencies utilize software that has been built following common cybersecurity practices.

Not too long ago, the only real criteria for the quality of a piece of software was whether it worked as advertised. With the cyber threats facing Federal agencies, our technology must be developed in a way that makes it resilient and secure, ensuring the delivery of critical services to the American people while protecting the data of the American public and guarding against foreign adversaries.

This is not theoretical: foreign governments and criminal syndicates are regularly seeking ways to compromise our digital infrastructure. In 2020, a number of Federal agencies and large corporations were compromised by malicious code that was added into SolarWinds software. This small change created a backdoor into the digital infrastructure of Federal agencies and private sector companies. This incident was one of a string of cyber intrusions and significant software vulnerabilities over the last two years that have threatened the delivery of Government services to the public, as well as the integrity of vast amounts of personal information and business data that is managed by the private sector.

# Why are we talking about this today?

- More to follow



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

September 14, 2022

M-22-18

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young Shalanda D. Young
Director

SUBJECT: Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

The Federal Government relies on information and communications technology (ICT) products and services to carry out critical functions. The global supply chain for these technologies faces relentless threats from nation state and criminal actors seeking to steal sensitive information and intellectual property, compromise the integrity of Government systems, and conduct other acts that impact the United States Government's ability to safely and reliably provide services to the public.

Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 12, 2021),[1] focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments. The EO directs the National Institute of Standards and Technology (NIST) to issue guidance "identifying practices that enhance the security of the software supply chain."[2] The NIST Secure Software Development Framework (SSDF), SP 800-218,[3] and the NIST Software Supply Chain Security Guidance[4] (these two documents, taken together, are hereinafter referred to as "NIST Guidance") include a set of practices that create the foundation for developing secure software. The EO further directs the Office of Management and Budget (OMB) to require agencies to comply with such guidelines. This memorandum requires agencies to comply with the NIST Guidance and any subsequent updates.

[1] Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[2] Executive Order on Improving the Nation's Cybersecurity (E.O.14028), Section 4(e)
[3] Available at: https://csrc.nist.gov/Projects/ssdf
[4] Available at: https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf

# Why open source?

Because it levels the playfield

- In Security we always have to assume that the adversary has complete access to the system, incluing code
  - Without Open Source, the defenders are fighting the fight their hands tied behind their backs
  - Defenders have to have access to the code without legal restrictions and/or limitations of technologies used

# Why open source?

Because it levels the playfield

- In Security we always have to assume that the adversary has complete access to the system, incluing code
  - Without Open Source, the defenders are fighting the fight their hands tied behind their backs
  - Defenders have to have access to the code without legal restrictions and/or limitations of technologies used

# Zero Trust Architecture

Tokens,tokens, everywhere

- Identity (for everything, not just humans)
  - Authentication
  - Authorization
    - Contextualized request
      - Validation of request against policies
      - Verification of behavioural references
    - Granting least privileges needed
      - Continuous verification and validation
      - Assumption that the granted entity can turn to be malicious
    - Automated degeneration of privileges at the earliest possible time
      - We still keep assuming, that who got the privileges can turn to be malicious
- Tokenization is the key to make this feasible
- And yet, tokens can be copied, spoofed, replay attacked, etc

# From Zero Knowledge Proofs to Zero Trust Architecture

What we are talking about?

- Innovation in security philosophy has been very limited, buzzwords came and went, but this time we are changing the fundamentals
  - Today we are "Trust, But Verify"
  - Zero Trust is "Never Trust Always Verify"
  - User, subjects, everyone is always assumed to be hostile
  - Edgeless network
  - Continuous verification
    - Tokenization of security
  - Contextualization of all request
    - Least permissions principle
  - Unfortunately large part of our security is still in "mainframe era"
    - Perimeter defence
    - Credentials driven
    - Trust by Authentication

# Authenticated should not mean the same as trusted

Those are two very different concepts

- Dr. Evil is still evil even after authenticating it is him
  - Sometimes you may want to talk with Evil, but why trusting?

- All Is Fair in Love and War (and stealing your assets online)
  - If brute force does not work, you are not using enough of it
  - … and get a better leverage

# The truth is in fiction

…especially in Cold War fiction

- Practice of Thinking Like the Enemy is really hard
    - Hint : The enemy thinks that they are the good guys
- Overwhelming majority of people who claim to be able to think like the enemy aren’t
    - They are thinking the way the would like to see the enemy to think
    - Critical Thinking is very rare
        - Deceiving yourself without even realizing that is not

# Critical thinking

…and why we suck at it

- Critical Thinking is unnatural for humans
  - We build communities and live in those
  - We love convenience
  - Building a community is fundamentally based on trust

Security systems inherit the flaw of overtrusting from the humans who created those

# It is all about the mindset

Everything is a weapon and an opportunity for a curious mind

- Unexpected surprise is what happens while you're waiting for the expected surprise
  - Think tanks and pundits specialize in expected surprise. (Surprise!)
- Give a man a zero-day and he'll have access for a day, teach a man to phish and he'll have access for life
  - The ultimate target is always the opponent's mind
    - Everything else is just technique
  - Impossible is just a state of mind

Even when the goal is to secure your enterprise systems, the starting point is not to hack it. The starting point is to understand the environment from the attacker's perspective and look for the weaknesses they see as exploitable, often completely ignoring the defenses you have built.

# Conclusions

- Zero Trust is a philosophy and methodology to address weaknesses technologies we have created have inherited from the human nature

  When you have to verify, there is no substitute to open source