Dr. Allan Friedman, National Telecommunications and Information Administration,
Department of Commerce, United States of America

EEF.DEL/46/18
6 September 2018

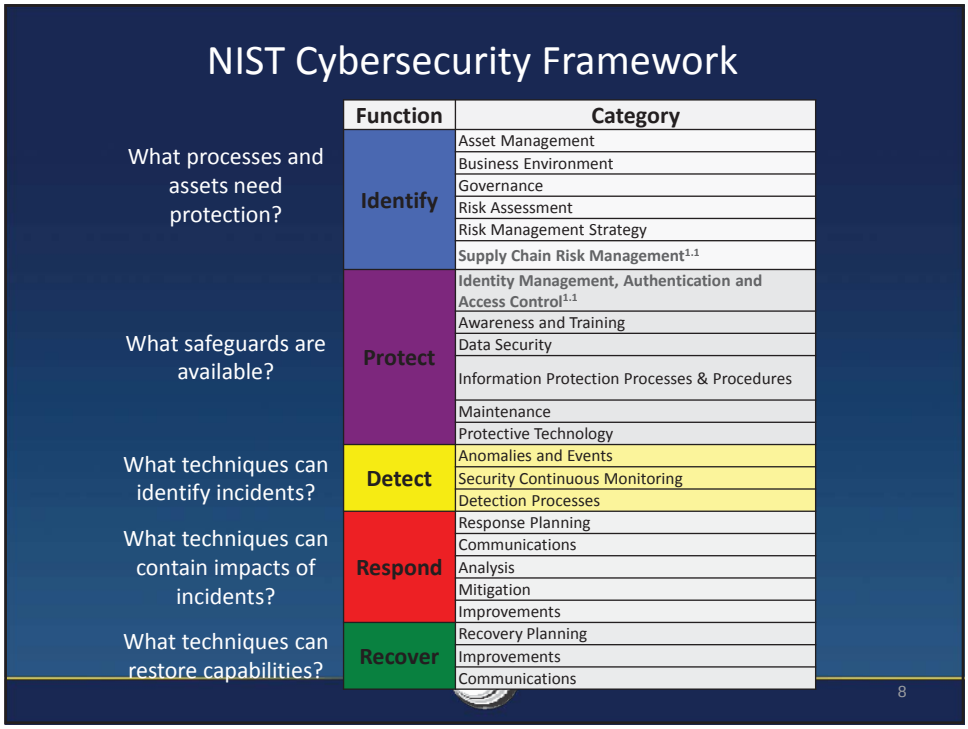
ENGLISH only

What does progress look like?
Improved security will come from changing behavior, driving investments, and using available tools

MAKE
things
Happen
Solutions come from market actors,
and will be implemented by market actors
Governments can help: Promote best practices.
Make it easier and cheaper to do the right thing

Some quick examples

NIST
Cybersecurity outcomes and informative references
Enables communication of cyber risk across an organization
CORE
TIERS
CYBERSECURITY FRAMEWORK
PROFILE
Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics
Aligns industry standards and best practices to the Framework Core in an implementation scenario
Supports prioritization and measurement while factoring in business needs
7


NIST Cybersecurity Framework
What processes and assets need protection?
What safeguards are available?
What techniques can identify incidents?
What techniques can contain impacts of incidents?
What techniques can restore capabilities?
Function
Category
Identify
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Supply Chain Risk Management[1.1]
Protect
Identity Management, Authentication and Access Control[1.1]
Awareness and Training
Data Security
Information Protection Processes & Procedures
Maintenance
Protective Technology
Detect
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Respond
Response Planning
Communications
Analysis
Mitigation
Improvements
Recover
Recovery Planning
Improvements
Communications
8

The Multistakeholder Model

Open, transparent, consensus based processes that bring together diverse stakeholders can catalyze real progress across the ecosystem.

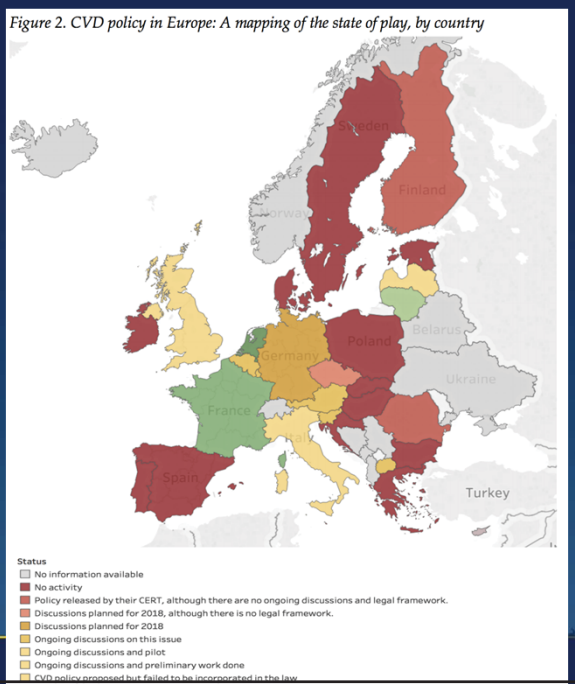
Vulnerabilities

Vulnerability Disclosure

No one likes being told their precious baby is not perfect

Vulnerability Disclosure: Template Disclosure Policy

Outcome: Stakeholder-drafted "early stages" template disclosure policy with a focus on safety-critical industries



Vulnerability Disclosure: A growing trend

Source: CEPS, 2018

13

Security: Where is the 'S' in '**IoT**'

As a starting point, we convened stakeholders to focus on "patchability," to foster an ecosystem that can be more resilient.

14

Software Component Transparency

15

Software Component Transparency

Transparency

Share Data

Vendors

Enterprise Customers

Compile Data

Use Data

Thank You!

afriedman@ntia.doc.gov