Third-party Security Validation: the Role of FIPS 140-2, Common Criteria, and UC APL in Securing Products (C11c).

Working Together To Secure Our Digital World

www.corsec.com // May 17, 2017

Security Validations: food for thought

Cyber Security for the Nation

To ensure that the internet remains valuable for future generations, [our policy is] to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft.

Presidential Executive Order

- That sentiment should be shared by government and industry alike.
- In fact, it should be an economically-incentivized sentiment.
- Consumers should see an economic benefit to investments in security for their devices, services, and infrastructure.
- But are they driven to purchase products with good security? And how would they know if they did?

How would you know?

- Buy from a reputable vendor. You can rely on them to provide a high level of security.
- Put your trust in a well-established company and brand with a good track-record and reputation.
- This is “first-party” assurance.

The limitation of first party assurance

- You can purchase from the best and biggest, and they may have good security. But that that does not reliably indicate you are protected
- In fact, it does not even ensure that we are protected with industry best-practice by default
- We all have first-person experiences that show that products with the best reputation may be less secure than lesser known products

Are Consumers Demanding Security

- Do Consumers try to get best-practice security when they purchase?

- Is there currently a difference between groups of consumers, for example, government and commercial?

What is Third-Party Assurance

- **Government relies on COTS products**
  - How can you tell if a COTS product is well built?
  - What differentiates “security in a bottle” from “snake oil” remedies?
  - What assurance can a vendor provide?
- **Assurance claims**
  - First Party Claim – The Vendor
    - (“Our products meet your needs” “Bulletproof security”.)
  - Second Party Claim – The Purchaser
    - (“This vendors products satisfy our requirements”)
  - Third Party Claim – Independent Evaluators
    - (“These products met these requirements”)

How do You Get Assurance?

Security Products, and their Cryptographic Engines are so complicated, how do we tell if they are designed and operating correctly? We need an inspection under the hood by qualified mechanics that we trust to tell us honestly what's going on there.

What programs do we have now?

The three largest, best-established programs:

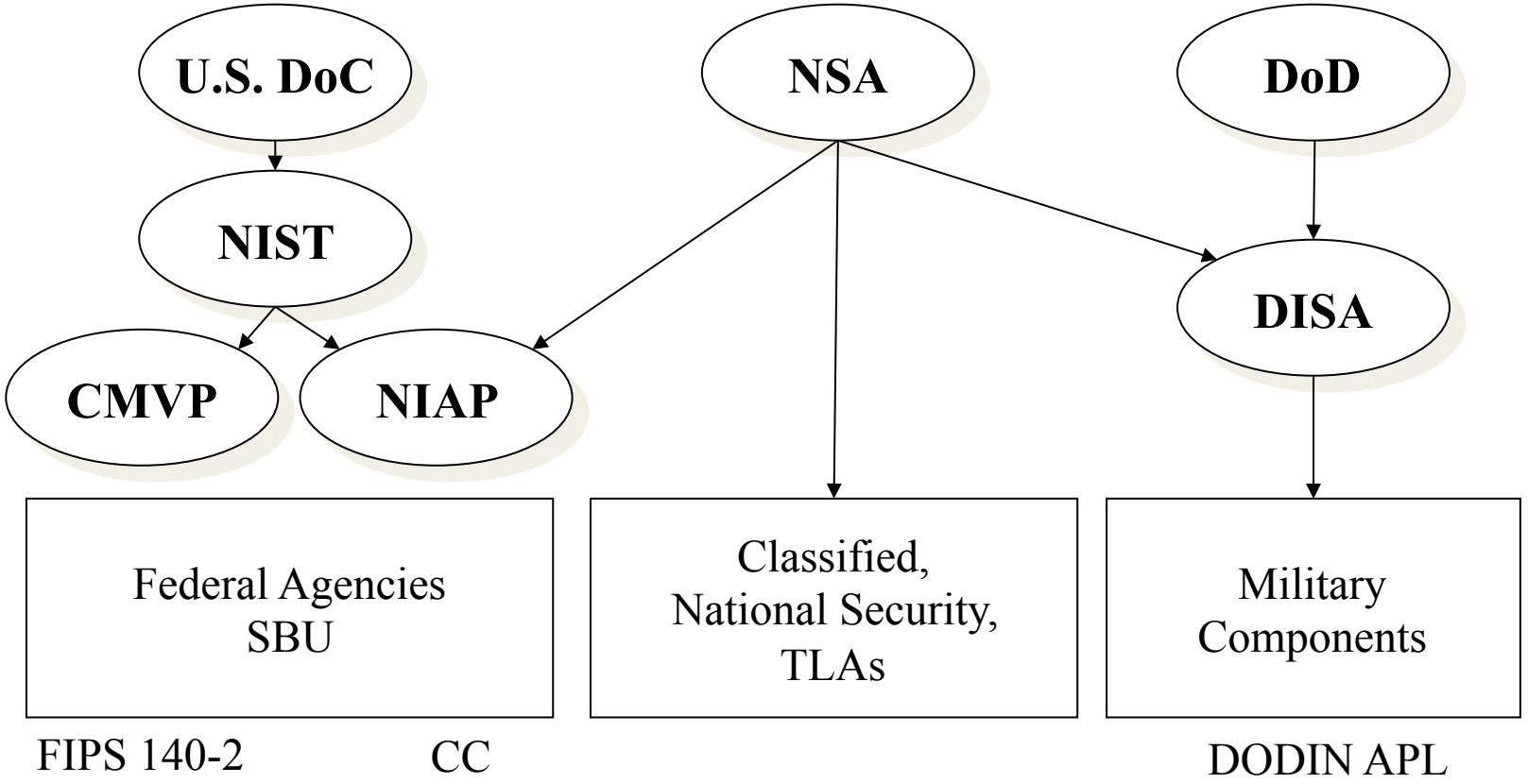
- FIPS 140-2
- Common Criteria
- DODIN APL

All share several key components, including

- Published criteria
- Third-party testing laboratories
- Accreditation bodies and process

A difficult landscape to deal with

Who has Aegis over what?



What Is FIPS 140-2

The Federal Information Processing Standard Publication 140-2:

- A U.S. and Canadian co-sponsored security standard
- Applies to hardware, software, and firmware products
- Required for products with cryptography if they are used in security systems that process Sensitive But Unclassified (SBU) information.

Mandates, Adoption, and Applicability

Mandates

- Applies to all U.S. federal agencies - mandated by law - Sect. 5131 of Information Technology Management Reform Act of 1996

Adoption

- Increasingly demanded in:
  - U.S. state and local government data systems
  - Emergency responders (police/fire/rescue)
  - Financial and healthcare industries
- Strictly enforced in Canada
- Global (European Union, South America, Asia, etc.)

Applicability

- A required component in Common Criteria certifications for products making cryptographic claims and a precursor to entry onto the Unified Capabilities Approved Products List (UC APL)

FIPS 140-2 Product Security Focus

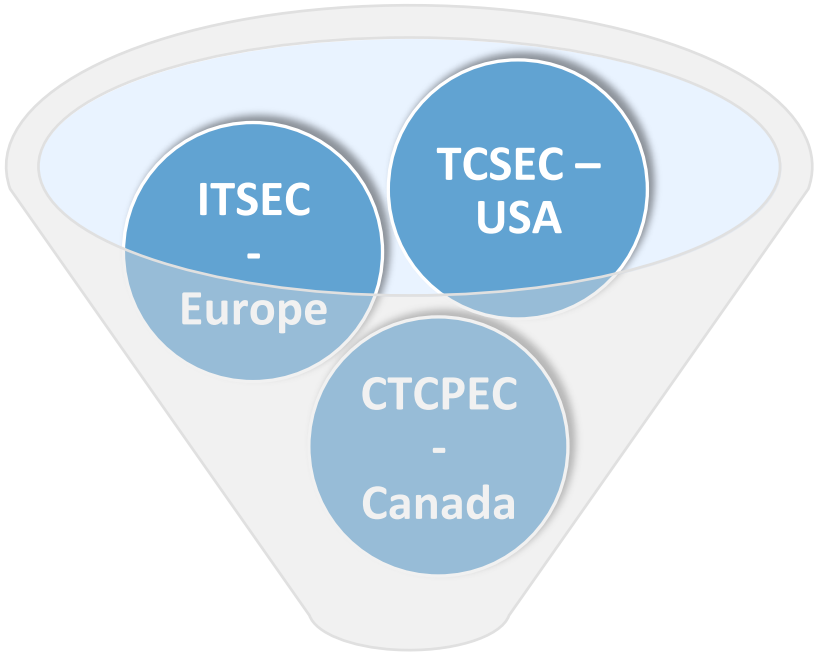
1. Cryptographic Module Specification
2. Module Ports and Interfaces
3. Roles, Services, and Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. Electromagnetic Interference / Electromagnetic Compatibility Testing (EMI/EMC)
9. Self-Tests
10. Design Assurance
11. Mitigation of Other Attacks

Common Criteria

“Common Criteria is a catalog of criteria, and a framework for organizing a subset of the criteria, into security specifications.”

- Internationally accepted
- Methodology for evaluating security features
- Can be applied to hardware, software, firmware, or a combination thereof
- Allows vendors to describes products’ security functionality with proof to support the claims

Common Criteria's International Origin



Common Criteria

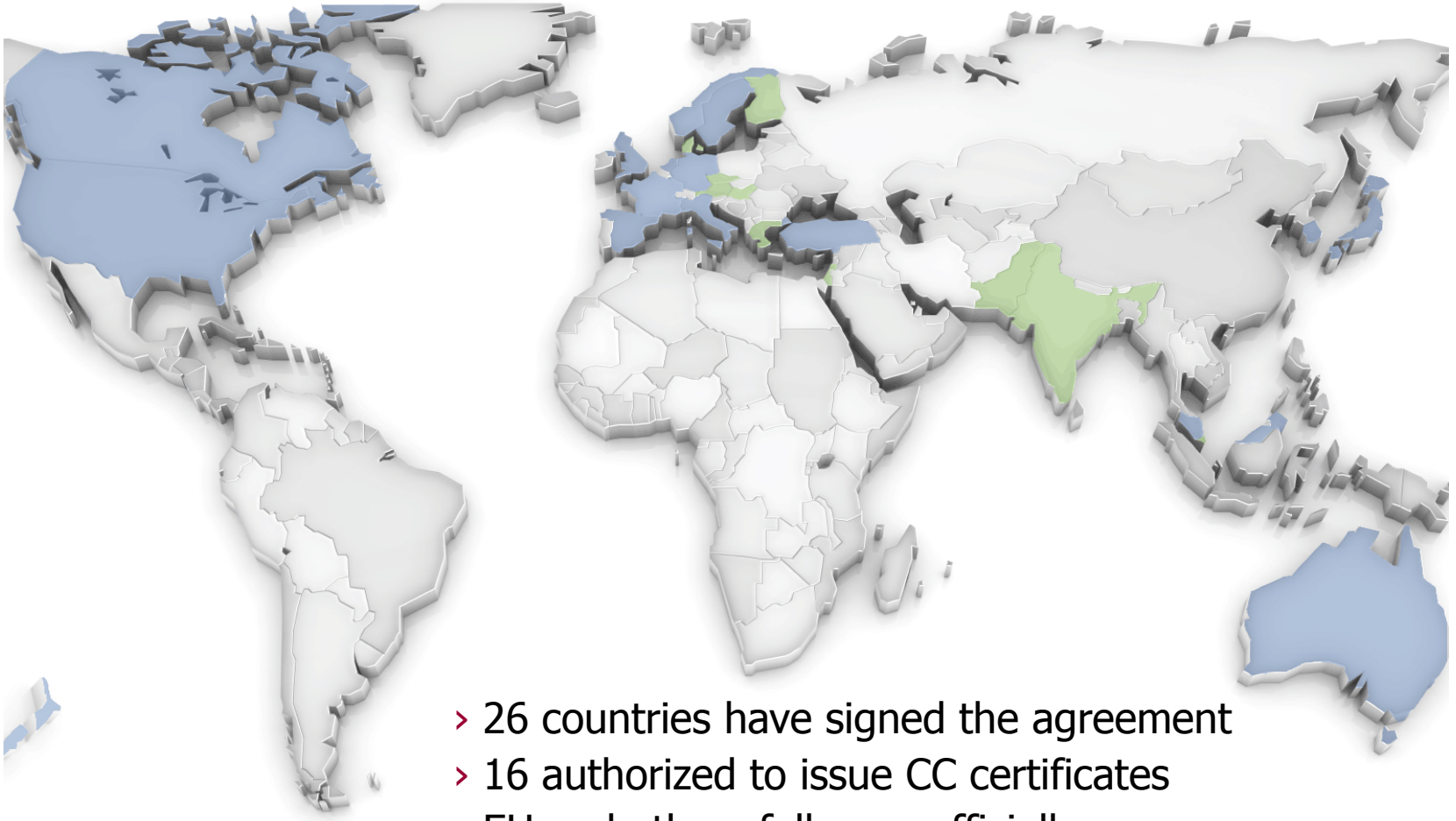
Now applicable to dozens of countries and appeals to multiple markets:

Government

Financial

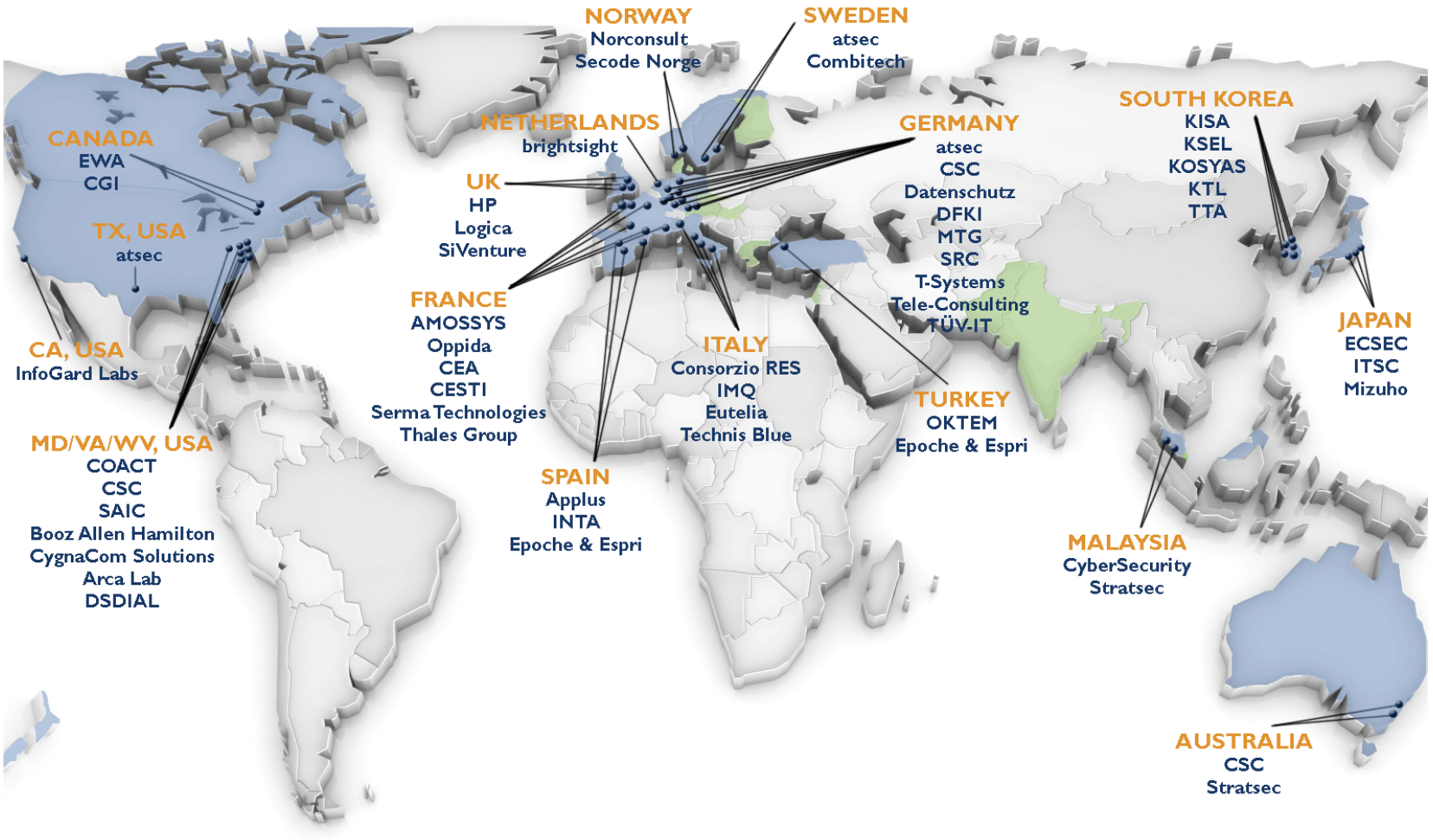
Healthcare

CCRA – Common Criteria Recognition Agreement



- 26 countries have signed the agreement
- 16 authorized to issue CC certificates
- EU and others follow unofficially

Independent Evaluation Labs



Common Criteria Focus Areas

CC Security Functional Requirements

- Audit (where logs are located, syslog capability, what is audited)
- Authentication (user attributes, types of authentication, password strength, any functions that are unauthenticated)
- Access control/Information flow control (data path attributes)
- Data protection (data integrity, encryption, etc.)
- Management (RBAC, management functionality)
- Trusted paths/channels
- High-availability/failover
- Self-protection
- Other security functionality (session timeouts, DoD access banner)

Development Lifecycle

- Source code and documentation revision control
- Delivery process (software, hardware, product verification methods)
- Flaw Remediation (bug tracking, regression testing, how are affected customers notified)

What Is The DODIN APL

The Department of Defense Information Network Approved Products List (DODIN APL)

- Formerly called the UC APL, the DODIN APL identifies solutions that are trusted to address government security concerns.
- The DODIN APL represents the agency's master list of products available for purchase that are secure, trusted and approved for deployment within the technology infrastructure.
- For all products that are implemented into the technology infrastructure of the U.S. DoD, the government is limited to purchasing only those solutions that have completed the DODIN APL process.

UC APL

US Army

US Air Force

US Marines

US Navy

Mandates, Applicability, and Key Considerations

Mandates

Required by DoDI 8100.04
Fulfills RMF IA Testing requirements

Applicability

Required for use on DoD Networks

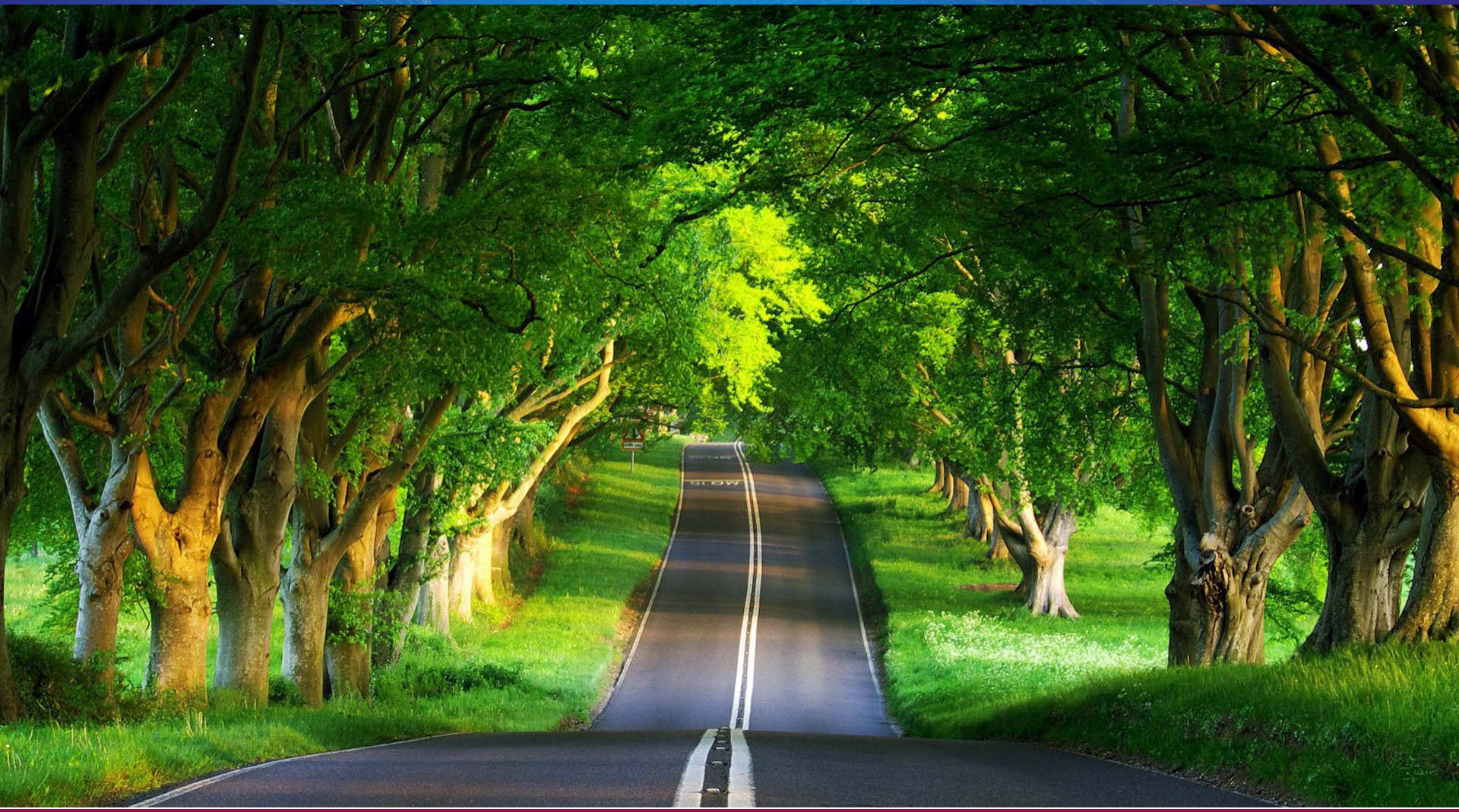
- Purchasers must purchase from DODIN APL first
- Many RFCs are requiring DODIN APL listing within a defined period

Builds on FIPS and CC certifications

Key Considerations

- Covers individual items that government purchasers request
  - » IPv6
  - » Common Access Cards

Finding the Right Path



How to Use Certifications

There only effective way to use certifications:

- Mandated requirement
- Enforced upon all vendors
- Backed-up by sufficient purchasing to justify costs (Commercially viable ROI)
- Consistently applied for long-enough for vendors to recoup investment
- Reviewed and updated to adjust to changing threat landscape

Assurance Limitations

Limitations of Programs:

- Cost and Complexity of Complying
- Cost and Complexity of Testing
- Lack of Product Security Improvement
- Lack of Feedback Circuit

Lack of Feedback Circuit

- What did we learn from Wannacry Ransomware?
- Do people say, if only folks were using certified products, this would not have happened.
- Does DODIN APL need a requirement to use only up-to-date, supported versions?
- Should Common Criteria address classes of attack that have previously caused zero-days?
- Where is the working group ensuring that FIPS, CC, and DODIN APL provide the best consumer protection given the currently reported hacks?
- Are we validating modules, products, or real-world deployable systems?

How Long Does it Take?

- How Long Does it Take?
  - How Long do you Have?
  - 9-36 months is typical to spend
  - The longer it goes, the less likely to finish
- What's the Cost of Longer?
  - One year of federal sales?
  - Market Share to Competitors?
  - Redoing work = higher costs
- Can you start selling it immediately?
  - In Evaluation, In Process, etc.
  - Education of Sales & Marketing

The Only Driver that Matters

You almost never hear the following:

"We don't have anything to spend our budget on this year, so we were thinking that maybe we could spend a few million working on FIPS 140-2 validations, CC evaluations, and UC APL listings over the next four quarters."

Money is a Huge Limitation

Benefits of Programs

Benefits of Programs (*if done correctly*)

- Designed to Ensure a Baseline of Security
- Make Security a Discriminator
- Vendors Invest in Improved Security
- Purchasers Can Source Secure Solutions
- Applicability of Program to Multiple Groups of Consumers

Additional Questions or Support?

John Morris| Corsec President

+1 (703) 267-6050 x105 | jmorris@corsec.com

About John:

John Morris is Corsec Security, Inc.'s President. For 19 years Corsec has assisted companies through the security certification and validation process. Corsec is a privately-owned company that partners with organizations worldwide to strengthen product security, improve brand reputation, and increase financial returns. Corsec's broad knowledge safeguards against common pitfalls and thwarts delays that derail most security certification projects.

Some of the Clients Corsec Serves


Corsec