Increasing the Value of Certifications to the End User

Jeffrey Blank

Vulnerability Solutions Office

NSA Cybersecurity

TALENT

TECH

TRUST

THREAT

Who is this End User?

In this context:

- Network owners
- Acquisition and risk decision makers
- Actual end users of IT products

…the people deploying and using the products

What does the End User want?

Things we hear most:

(1) To use products that best meet their needs
(2) Efficiencies in network accreditation
(3) Confidence in new technology paradigms

Let’s see how we’re doing

Products that best meet needs

- Speed, speed, and speed of evaluation is key

  Did I mention SPEED? There are points of light here

    - NIST’s strategy for automated module testing
    - NIAP’s 90-day evaluation mantra

- Innovation in creating new requirements documents

  - e.g. GitHub

- Explicit non-involvement of certification bodies in product spaces not suited for certification

  Is more clarity needed?

Efficiencies in Network Accreditation

- In the US, NIST maintains a Risk Management Framework for accrediting *information systems*
  - NIST SP 800-53 provides a catalog of security controls
- NIAP provides mappings of NIST controls for each PP
  - This provides confidence that the security functionality has been evaluated, in validated products

Efficiencies in Network Accreditation

- Knowing what’s on the network is essential to accreditation or assessment of a network
- This is one of NSA’s Top 10 Mitigations and one of CIS’s Basic Controls
- Certain NIST 800-53 controls are also required by CNSSI 1253, *including the validation of IT components against a NIAP-approved Protection Profile*
    - Insight into the level of operational compliance should be very informative to us!

Efficiencies in Network Accreditation

- Other controls are achieved by implementing certain configuration settings for individual IT products
    - Address this need by producing operationally-useful guidance as part of CC and FIPS evaluations
    - NIAP will be posting *Configuration Annexes* to assist vendors and labs in this process
    - This will also address the problem of configuration guides masquerading as product approval

Confidence in New Technology

- “The Cloud” – not a new concept in 2018
  - Component vs system: FIPS, CC, FedRAMP
  - Which components?
- Quantum cryptography
- Authentication mechanisms
- Internet of Things?

One Last Thing

- Clarity.

  There are a variety of other certification approaches that come and go.

  This creates ongoing confusion for the end user, as well as industry.

  We can manage this confusion together.