Trusted Computing

IAD Forward. Thinking.

INFORMATION ASSURANCE DIRECTORATE

Standards Overview

Mike Boyle
IAD Technical Lead for Standards

WHAT IS A TECHNICAL STANDARD?

- A **technical standard** is an established norm or requirement about technical systems. It is usually a formal document that establishes uniform engineering or technical criteria, methods, processes and practices.
- Typical Characteristics
  - Created through a standards body whose members represent a number of different organizations
  - Established in order to meet technical, safety, regulatory, societal and market needs
  - Catalysts for technological innovation and global market competition

SAMPLE STANDARDS BODIES

- Trusted Computing Group (TCG) – secure hardware core and trusted computing protocols
- Internet Engineering Task Force (IETF) – standard security protocols and implementations
- Distributed Management Task Force (DMTF) – systems management in enterprise IT environments
- Institute of Electrical and Electronics Engineers (IEEE) – wide range of industries including energy, healthcare, Information Technology (IT), telecommunications, and many more
- International Organization for Standardization (ISO) – proprietary, industrial, and commercial standards
- National Institute of Standards and Technology (NIST) – measurement science, standards, and technology

WHY DO WE HAVE STANDARDS?

- **Standards reduce costs for customers and manufacturers – they serve a business need**
- Standards may be created to:
  - Facilitate interoperability
  - Limit the variety of implementations
  - Enable verification of compliance
  - Specify minimum security or functional requirements
  - Publicly express market/business needs

THE BOTTOM LINE – STANDARDS REDUCE COSTS

- Custom solutions are expensive
  - The cost of building custom solutions that keep pace with global technology change has been growing exponentially
  - The cost of custom solutions increases over time as changes need to be made
- Standards create leverage
  - When standards are agreed upon, there is often market pressure for vendors to comply
  - It is often easier to influence standards and far less costly than to individually drive vendors to modify their products

AND THE POINT IS?

- When your requirements do not map into any accepted standard, you have a choice to make:
  1. Pay to have custom work done to meet your requirements
  2. Do without a solution to your requirements
  3. Take an active role in the Standards process to lobby for solutions that satisfy your requirements

Acquisitions create products – standards create ecosystems

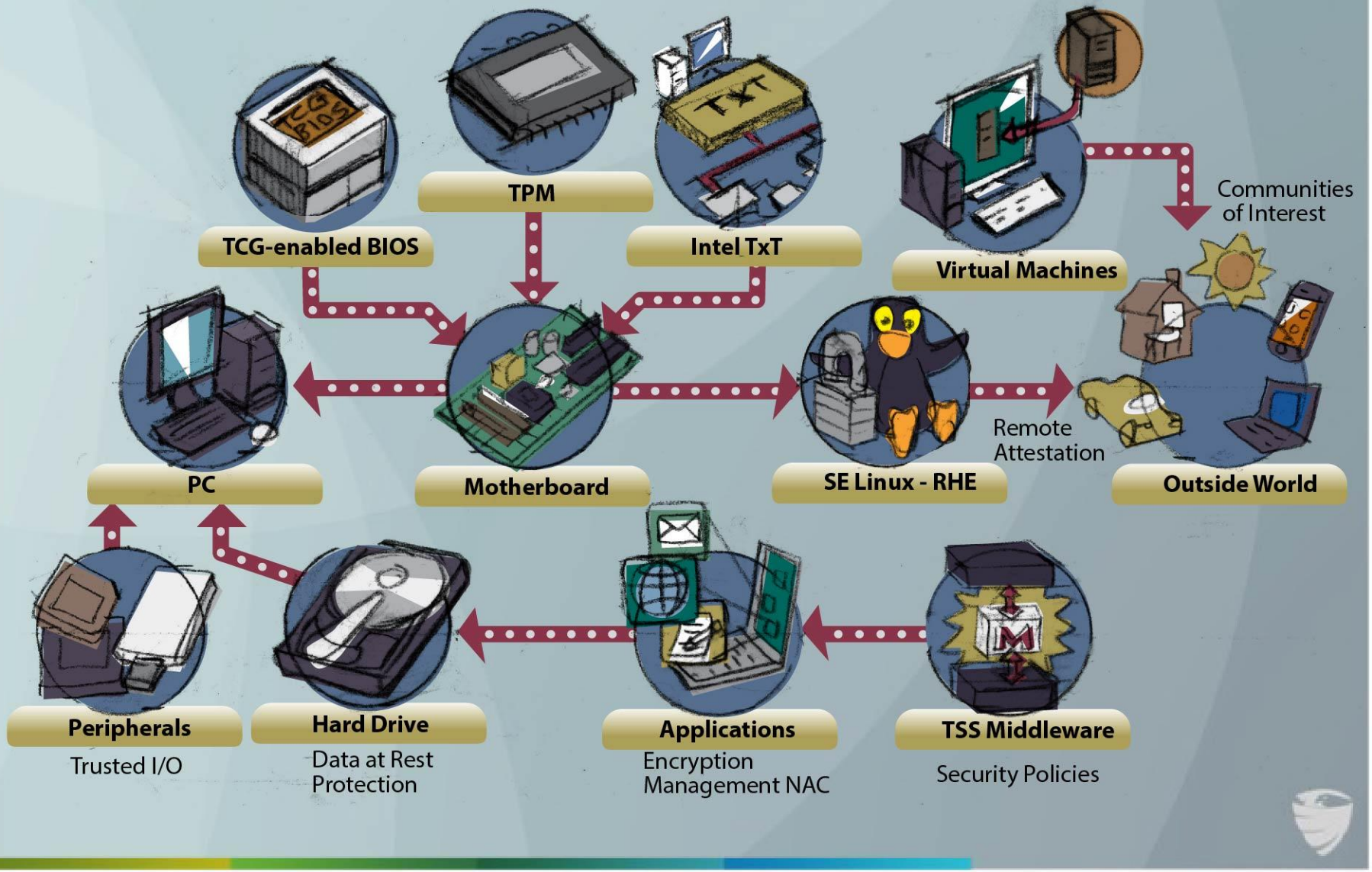
USG, CYBERSECURITY AND STANDARDS – A HISTORY LESSON

- In the past, the USG has had to pay for custom solutions to meet their needs, however
  - The line is blurring between commercial need and government need for security
  - Industry solutions are getting closer to meeting needs for higher-assurance government applications
  - It is too expensive to pay and maintain custom solutions

ENTER THE TRUSTED COMPUTING GROUP (TCG)

- The Trusted Computing Group (TCG) , a standards body comprising more than 100 companies, developed an industry specification called the Trusted Platform Module (TPM) , which enables trust in computing platforms via the hardware
- TPM is the foundation for an entire ecosystem
- Very few documents for the TPM standards itself
  - TPM specification v1.2 was accepted by JTC1 (a joint committee of the International Organization for Standardization, or ISO, and IEC, the International Electrotechnical Commission) and published as ISO/IEC Standard 11889 in 2009
  - The TPM 2.0 specification is currently in development, and the TCG Work Group expects it to be completed by mid-year
- But the TPM standard drove the creation of an entire ecosystem on PCs . . .

THE TPM ECOSYSTEM FOR PC



USG, CYBERSECURITY AND TCG STANDARDS – A HISTORY LESSON

- *Early 2000*
  - TCG releases TPM specification
  - USG recognized hardware-based security solutions, like the TPM, would be beneficial to cybersecurity, but did not get involved in developing the specification
- *2003*
  - The TPM v1.2 specification closed with very little input from the US Government
  - TPM v1.2 does not easily meet the Federal Information Processing Standard (FIPS)-140-2 certification requirements (lots of reasons), thus does not fully meet the standards needed by the USG
    - Federal Information Processing Standards (FIPS) standards provide guidance for federal information systems
    - FIPS 140-2 sets the standard for cryptography on those systems

IT'S A MATTER OF CHOICE

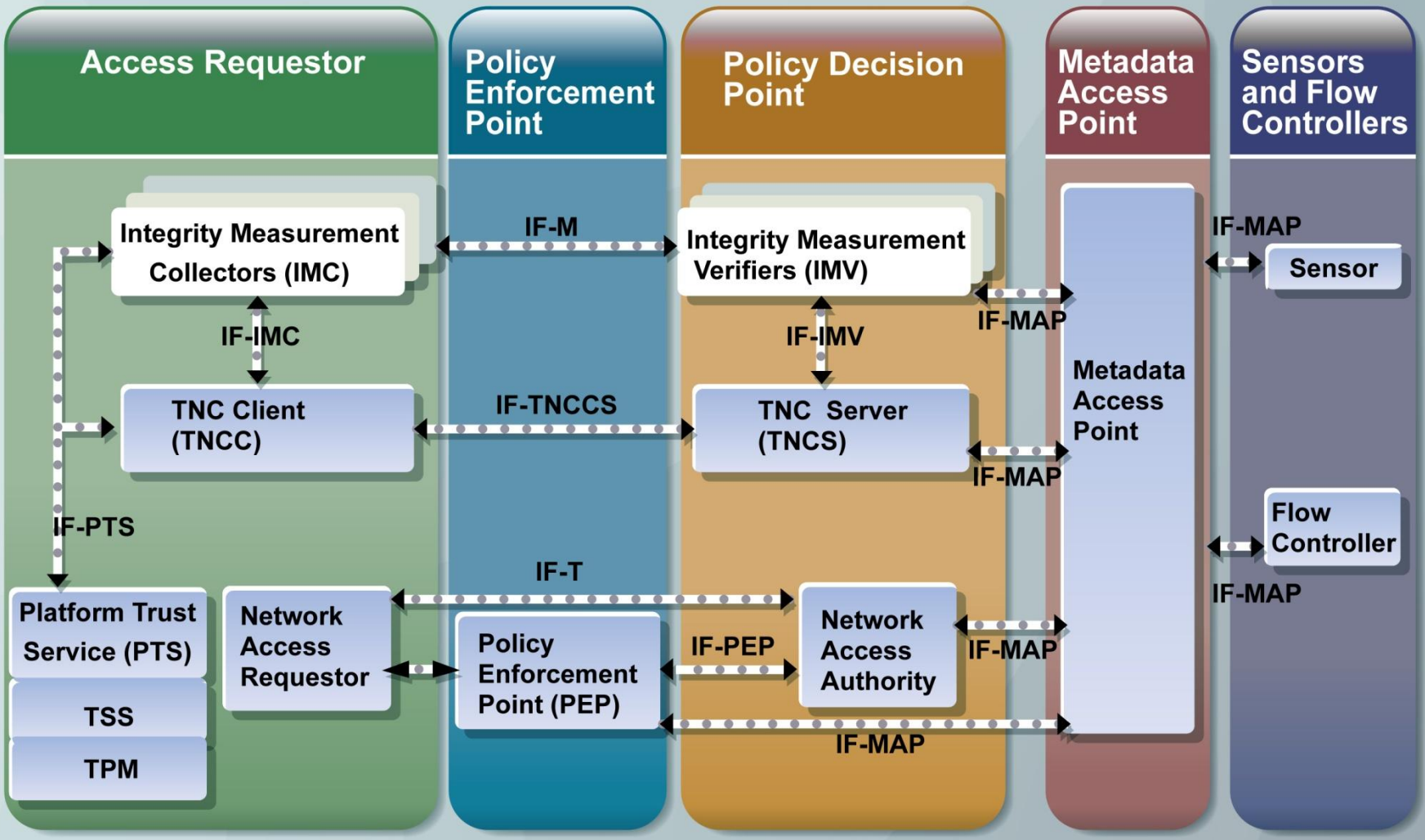
- As stated earlier, when a standard does not meet your need, you have three choices:
  1. Pay to have custom work done to meet your requirements
  2. Do without a solution to your requirements
  3. Take an active role in the Standards process to lobby for solutions that satisfy your requirements

USG decided to chose option #3 and get involved

THE RESULT

- *Today*
  - The National Security Agency (NSA) and NIST are actively participating with the TCG to develop the TPM 2.0 specification, which will likely result in FIPS 140-2 or 140-3 certification
  - Currently NSA lab are testing products for interoperability regarding TCG's Trusted Network Connect (TNC) standards
  - NSA worked with TCG's Storage Working Group (WG) to create protection profiles for self-encrypting drives (SEDs)

USG TESTING OF THE TNC ECOSYSTEM



http://www.trustedcomputinggroup.org/developers/trusted_network_connect/specifications

USG AND SED STANDARDS

- TCG's Opal Security Subsystem Class Specification offers a set of mechanisms and protocols for disk-drive encryption, authentication, configuration, and policy management for storage devices used in the PC client and enterprise markets
- TCG's Enterprise Security Subsystem Class Specification extends the concepts of trusted storage devices to those used in data centers and high-volume applications
- ***Remember: USG's requirements for "sensitive but unclassified" data are specified in FIPS 140-2***
  - Interplay between commercial standards and testing

AND THE PARTICIPATION TREND IS GROWING

- Commercial Solutions for Classified Program (CSFC)
  - Represents a recognition that commercial solutions can be an important component in the protection of highly sensitive data
  - Provides a new avenue for vendors to provide products that meet both government and commercial needs
- High Assurance Platform (HAP) Program
  - Proof-of-concept that high-assurance, multi-domain solutions can be built from commercial-off-the-shelf (COTS) components
- Major Commercial Security Standards Initiatives
  - Internet Engineering Task Force (IETF) – Standard security protocols and implementations
  - Distributed Management Task Force (DMTF) – Systems management in enterprise IT environments

PARTICIPATION LEVEL BASED ON NEED

- ***Lesson learned: Joining the standards groups allows you to promote your interests***
  - In cybersecurity, especially when hardware is involved, USG interests are often well served by ***active, coordinated*** participation in relevant standards bodies
- Participation in a Standards body can be active or passive
  - **Passive**: observe work being done, report to your organization
    - This approach works well when the market or an active participant in the Standards body is a driving force
  - **Active**: volunteer in the creation of a standard
    - Doing the work means you have more influence to shape the direction and content of the specification
    - Most powerful positions in the Working Group: Editor and Chair
      - Editor: "The Pen is mightier than the Sword" – you write the spec
      - Chair: Sets the agenda

Whether participation is active or passive, if you have features you need in a standard, you need to participate.

WHERE TO START?

- First – determine the need
  - Know what problems matter the most to you
  - Discover what standards organizations are actively addressing those problems
  - Pick the right work groups in the standards group
- Next – determine an effective approach
  - If the topic is sufficiently important, look at direct involvement
  - Coordinate with those already participating in the group
  - If needed, pick people with the right skills to join the group
  - Make it a priority to be active in the working groups (WG) – those who do the most work often get the best results
  - Set goals for results in the WG

BOTTOM LINE

- Joining standards group provides an organization, including USG, the opportunity to actively participate in the creation of solutions that meet its needs
- To maximize its influence, the USG needs to:
  - Agree on the technologies that are needed
  - Speak with one voice to encourage development of standards that define those technologies
  - Procure the technologies that meet those standards and implement them across USG

QUESTIONS?