1. Why a standard?
2. How to choose the best standard?
3. Public and private roles?
A Computer Security Incident = A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Source: SP 800-61

For us:

Indicator == observable-event-info + context-info

1. We are developing SP800-150, providing guidance on safe, effective information sharing.
2. This will supplement existing NIST guidance on incident handling, SP 800-61.

*Supported by DHS.*
We are releasing an RFI as part of Incident Coordination due diligence.

We have held general conversations with practitioners.

A few observations (not consensus):

- SIMPLE facilitates sharing; COMPLEX impedes sharing. many-screens == bad cheap-tools == good
- DCISE: 80+ element xml schema and ZERO adoption, even by the authors.
- A decline of average-maturity is natural as a community grows.
- Expanded CSV is practical: (indicator, type, role, attack-phase, comments).
- A taxonomy regarding roles and types is defined but closely held.
- HARD PROBLEM: establishing trust relationships in a circle of sharing.

Organizational maturity varies a lot.

Estimating both trust and report-quality is currently subjective: have to work with this.

An indicator file reveals what we can see.

Disclaimer: any mention of companies, products, or services does not imply endorsement.
Why a “realistically ambitious” Standard?

• **Lots of reasons:**
  – To support important use cases, not fascination with mechanisms.
  – To define quality: good-enough indicators.
  – To foster a market of indicator producers, consumers, and tools.
  – For interoperability, portability, speed.
  – To increase the feasibility of automation: less unstructured text helps; but probably can’t get rid of it.
  – To scale a defense of critical infrastructure.
  – To foster a common data model.
  – To reduce costs of CSIRTs.

• **However:**
  – Attack landscape is evolving, and **guidance** may be more durable and actionable than a complex standard.
  – Hard Problems such as **trust**, **procedure**, **legal issues** are difficult to address with techie-driven standards.
  – NO handcuffs please!
How to Choose the Best Standard?

- **Use cases** should drive (actors; steps).
- **SIMPLE** facilitates sharing; **COMPLEX** impedes sharing.
- Support **incremental** adoption: training-wheels mode.
- Support easy **grep**-like search-based access.
- Prefer low **schema** complexity.
- Work across organizations with different **maturity** levels.
- Relate to open **legacy** tools (e.g., Snort rules).
- Scalable to many **thousands** of participants.
- Support **reputation** maintenance and info vetting.
- **Extensibility.**
Public and Private Roles

• **NIST:**
  – Release guidance.
  – Facilitate open, consensus-based standards.
  – Technology-neutral.
  – Industry led if possible.
  – Competitions
  – NCCoE: collaborating with industry
    • leveraging existing commercially available capabilities to generate solutions to hard problems

• **Private Entities:**
  – Preferred: lead standards efforts.
  – Validate standards concepts via prototypes/products.
Team Members

• NIST
  – Lee Badger, David Waltermire
• DHS
  – Tom Millar
• G2
  – Greg Witte, George M. Saylor, Matthew Smith
• MITRE
  – Clem Skorupta, Rick Murad, Karen Quigg,